VORLESUNGEN

ÜBER

ZAHLENTHEORIE

VON

P. G. LEJEUNE-DIRICHLET.

HERAUSGEGEBEN

VON

R. DEDEKIND.
Professor am Collegium Carolinum zu Braunschweig.

BRAUNSCHWEIG,
DRUCK UND VERLAG VON FRIEDRICH VIEWEG UND SOHN.
1863.



VORLESUNGEN

ÜBER

ZAHLENTHEORIE

VON

P. G. LEJEUNE-DIRICHLET.

VORLESUNGEN

ÜBER

ZAHLENTHEORIE

VON

P. G. LEJEUNE-DIRICHLET.

HERAUSGEGEBEN

VON

R. DEDEKIND,
Professor der höheren Mathematik am Collegium Carolinum zu Braunschweig.

BRAUNSCHWEIG,
DRUCK UND VERLAG VON FRIEDRICH VIEWEG UND SOHN.
1863.



VORWORT DES HERAUSGEBERS.

Gleich nach dem Tode Dirichlet's wurde ich mehrfach aufgefordert, die von ihm gehaltenen Universitäts-Vorlesungen, welche so ausserordentlich viel zur Verbreitung der Bekanntschaft mit neueren und feineren Theilen der Mathematik beigetragen haben, in möglichst getreuer Form zu veröffentlichen; ich glaubte dieser Aufforderung um so eher nachkommen zu können, als ich in den Jahren 1855 bis 1858 die wichtigsten dieser Vorlesungen in Göttingen gehört und ausserdem vielfach Gelegenheit gehabt hatte, im persönlichen Verkehr Dirichlet's Gründe für die von ihm befolgte Methode des Vortrags kennen zu lernen. Nachdem auch die Verwandten Dirichlet's mich dazu ermächtigt haben, so übergebe ich dem mathematischen Publicum hiermit eine Ausarbeitung der Vorlesung über Zahlentheorie, bei welcher im Wesentlichen der im Winter 1856 bis 1857 von Dirichlet befolgte Gang eingehalten ist; er selbst fasste damals den Gedanken einer Herausgabe dieser Vorlesungen, und da er seinen

Vortrag nie schriftlich ausgearbeitet hatte, so diente ihm ein von mir geschriebenes, allerdings nur die Hauptmomente der Beweise enthaltendes Heft dazu, einen ungefähren Ueberschlag über die Ausdehnung der einzelnen Abschnitte zu machen. In öfter wiederkehrenden Gesprächen über diesen Plan äusserte er die Absicht, bei der Veröffentlichung manche Abschnitte hinzufügen zu wollen, die in einem Lehrbuch nicht fehlen dürften, die aber in jener Winter-Vorlesung aus Mangel an Zeit übergangen werden mussten. Bei der jetzigen Herausgabe ist daher im Wesentlichen zwar das eben erwähnte Heft zu Grunde gelegt, aber ich habe theils nach älteren Heften, theils nach Dirichlet'schen Abhandlungen, endlich auch ganz nach eigenem Ermessen Zusätze von nicht unbedeutender Ausdehnung gemacht, welche ich hier anführen zu müssen glaube, um für sie die Verantwortlichkeit zu übernehmen; sie sind in den Paragraphen 105 bis 110, 121 bis 144 und in den unmittelbar unter den Text gesetzten Anmerkungen enthalten.

Es ist meine Absicht, diesem ersten Bande, dessen Vollendung durch andere Arbeiten sich bis jetzt verzögert hat, zunächst einen zweiten weniger umfangreichen nachfolgen zu lassen, in welchem die Vorlesung über die im umgekehrten Verhältniss des Quadrats der Entfernung wirkenden Kräfte wiedergegeben werden soll.

Braunschweig, im October 1863.

R. Dedekind.

INHALT.

Seite

Vierter Abschnitt: Von den quadratischen Formen.

Seite

Fünfter Abschnitt: Bestimmung der Anzahl der Classen, in welche die binären quadratischen Formen von gegebener Determinante zerfallen.

Supplemente.

Erster Abschnitt.

Von der Theilbarkeit der Zahlen.

§. 1.

Wir behandeln in diesem Abschnitte einige arithmetische Sätze, welche man zwar in den meisten Lehrbüchern vorfindet, die aber für unsere Wissenschaft von so fundamentaler Bedeutung sind, dass eine strenge Begründung derselben hier durchaus nothwendig erscheint. Dahin gehört zuerst der Satz, dass das Product einer Reihe von ganzen positiven Zahlen unabhängig von der Anordnung ist, in welcher man die Multiplication ausführt. Indem wir uns zunächst auf den Fall beschränken, in welchem es sich um *drei* Zahlen a, b, c handelt, bilden wir das folgende Schema

$$\begin{matrix} c, & c, & c, & c \dots c \\ c, & c, & c, & c \dots c \\ c, & c, & c, & c \dots c \\ \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots \\ c, & c, & c, & c \dots c, \end{matrix}$$

welches aus b Horizontalreihen besteht, deren jede die Zahl c gleich oft, nämlich a mal enthält, und stellen uns die Aufgabe, die Summe aller aufgeschriebenen Zahlen zu bestimmen. Zunächst können wir sagen: da die Zahl c in jeder Horizontalreihe a mal vorkommt, so ist nach dem Grundbegriff der Mul-

tiplication die Summe aller in einer solchen Reihe befindlichen Zahlen gleich ca, indem wir den Multiplicand c durch die Stellung von dem Multiplicator a unterscheiden; da ferner b solche Horizontalreihen vorhanden sind, so ist die Summe sämmtlicher Zahlen gleich $(ca)b$, wo jetzt ca der Multiplicand, b der Multiplicator ist. Nun können wir aber dieselbe Summe auch auf anderm Wege durch die Bemerkung bestimmen, dass das obige Schema aus a Verticalreihen besteht, deren jede b mal die Zahl c enthält; es ist also die Summe aller in einer Verticalreihe befindlichen Zahlen gleich cb, und folglich die Totalsumme gleich $(cb)a$. Wir erhalten mithin das erste Resultat

$$(ca)\,b = (cb)\,a,$$

aus welchem wir, indem wir die bisher ganz willkürliche Zahl $c = 1$ setzen, die Folgerung ziehen, dass

$$ab = ba$$

ist, d. h. dass in einem Product aus zwei ganzen positiven Zahlen Multiplicand und Multiplicator mit einander vertauscht werden dürfen. Man lässt deshalb auch in der Benennung den Unterschied zwischen Multiplicand und Multiplicator ganz fallen, indem man beide unter dem gemeinschaftlichen Namen Factoren zusammenfasst.

Wir können nun dieselbe Totalsumme sämmtlicher in dem obigen Schema befindlichen Zahlen noch auf eine dritte Art bestimmen, indem wir abzählen, wie oft der Summand c im Ganzen vorkommt. Zunächst ist a die Anzahl der in einer jeden Horizontalreihe befindlichen Zahlen c, und folglich ist, da b solche Horizontalreihen vorhanden sind, die Anzahl aller aufgeschriebenen Zahlen gleich ab. Hieraus folgt, dass die Totalsumme den Werth $c(ab)$ hat, dass also

$$(ca)b = (cb)a = c(ab)$$

ist. Verbindet man hiermit den schon oben betrachteten speciellen Fall $ab = ba$, so kann man das Bisherige in folgendem Satze zusammenfassen:

Wenn man von drei positiven ganzen Zahlen zwei nach Belieben auswählt und als Factoren zu ihrem Producte vereinigt, sodann dieses Product und die dritte jener drei Zahlen mit einander multiplicirt, so hat das so entstehende Product stets den-

selben Werth, wie man auch die ersten beiden Zahlen ausgewählt haben mag.

Da also dieses Product von der Anordnung der beiden successiven Multiplicationen ganz unabhängig ist, so bezeichnet man dasselbe kurz als das Product aus jenen drei Zahlen und nennt diese letzteren ohne Unterschied die Factoren des Productes.

§. 2.

Es ist nun leicht zu zeigen, ohne ein neues Princip anzuwenden, dass ein ganz ähnlicher allgemeinerer Satz für jedes System S von beliebig vielen positiven ganzen Zahlen

$$a, \; b, \; c \; . \; . \; .$$

gilt. Die allgemeinste Art, diese Zahlen durch wiederholte Anwendung einfacher, d. h. auf nur zwei Zahlen bezüglicher Multiplicationen zu einem Producte zu vereinigen, ist folgende. Man greife nach Belieben zwei Zahlen aus dem System S heraus und bilde ihr Product; der aus den übrigen Zahlen des Systems S und aus diesem Product bestehende Zahlencomplex S' enthält dann eine Zahl weniger als S; indem man wieder ganz nach Belieben zwei Zahlen aus S' zu ihrem Producte vereinigt und die anderen unverändert lässt, erhält man ein System S'' von Zahlen, deren Anzahl um zwei kleiner ist als die der ursprünglich gegebenen Zahlen. Fährt man so fort, so wird man zuletzt zu einer einzigen Zahl gelangen, und der zu beweisende Satz besteht darin, dass diese am Ende des Processes resultirende Zahl immer dieselbe sein wird, auf welche Art man auch die einzelnen einfachen Multiplicationen anordnen mag.

Um dies zu zeigen, wenden wir die vollständige Induction an, d. h. wir nehmen an, der Satz sei richtig, wenn die Anzahl der ursprünglich gegebenen Zahlen oder Factoren $= n$ ist, und beweisen, dass er dann auch für die nächst grössere Anzahl $n+1$ von Factoren ebenfalls gültig sein muss. Es sei also ein System S von $n+1$ Zahlen

$$a, \; b, \; c, \; d, \; e \; . \; . \; .$$

gegeben, so wähle man irgend zwei derselben, z. B. a und b, und bilde ihr Product ab; der nun entstehende Zahlencomplex enthält nur noch die n Zahlen

$$ab, \ c, \ d, \ e \ . \ . \ .$$

und folglich ist nach unserer Annahme das Endresultat von der weiteren Anordnung des Processes ganz unabhängig. Bei einer andern Anordnung der ganzen Operation kann daher höchstens dann ein anderes Endresultat zum Vorschein kommen, wenn das bei dem ersten Schritte ausgewählte Zahlenpaar von a, b verschieden ist, und zwar sind zwei Fälle zu unterscheiden.

Erstens kann es sein, dass bei der zweiten Anordnung zuerst *eine* der beiden Zahlen a, b, z. B. a, mit einer der übrigen $c, d, e \ldots$, z. B. mit c, zu dem Producte ac vereinigt wird, so dass der nächste Complex aus den n Zahlen

$$ac, \ b, \ d, \ e \ . \ . \ .$$

besteht; da nun sowohl bei der ersteren, wie bei der letzteren Anordnung die auf den ersten Schritt folgenden Operationen keinen Einfluss auf das Endresultat ausüben können, so setze man die erste Anordnung so fort, dass zunächst die beiden Zahlen ab und c, die zweite so, dass zunächst die beiden Zahlen ac und b vereinigt werden. Auf diese Weise entsteht bei der ersten Anordnung zunächst der Complex

$$(ab)c, \ d, \ e \ . \ . \ .$$

bei der zweiten der Complex

$$(ac)b, \ d, \ e \ . \ . \ .$$

Da nun zufolge des vorhergehenden Paragraphen die beiden Producte $(ab)c$ und $(ac)b$ und folglich auch die beiden vorstehenden Complexe identisch sind, so wird, da jeder derselben nur noch $n - 1$ Zahlen enthält, bei der ersten, wie bei der zweiten Anordnung dasselbe Endresultat auftreten.

Zweitens kann es aber auch sein, dass bei dem ersten Schritt der zweiten Anordnung *keine* der beiden Zahlen a, b, sondern zwei von den übrigen, z. B. c, d, herausgegriffen werden, so dass zunächst der Complex

$$a, \ b, \ cd, \ e \ . \ . \ .$$

entsteht. Auch jetzt kann man wieder die auf den ersten Schritt folgenden Operationen bei beiden Anordnungen nach Belieben ausführen; man vereinige daher zunächst bei der ersten Anordnung die Zahlen c, d, und bei der zweiten Anordnung die Zah-

len a, b; dann besteht bei beiden Anordnungen der nächstfolgende Complex aus denselben $n-1$ Zahlen

$$ab,\ cd,\ e\ \dots$$

und folglich wird abermals das Endresultat bei beiden dasselbe sein.

Hiermit ist die Allgemeingültigkeit des Satzes bewiesen; denn da er nach dem vorhergehenden Paragraphen für $n=3$ gilt, so gilt er nach dem Vorstehenden auch für alle Systeme von Zahlen, deren Anzahl $=4, 5, 6$ u. s. w. ist. Das Endresultat heisst auch jetzt wieder das Product aus den gegebenen Zahlen, diese letzteren heissen die Factoren des Productes, und man bezeichnet das Product durch das Nebeneinanderschreiben sämmtlicher in beliebiger Ordnung folgenden Factoren.

Ein besonderer Fall dieses Satzes ist der, dass man bei der Bildung des Productes aus beliebig vielen Zahlen oder Factoren dieselben nach Belieben in Gruppen vertheilen und alle in einer Gruppe enthaltenen Factoren zu ihrem Product vereinigen darf; das Product aus diesen den einzelnen Gruppen entsprechenden Producten wird immer mit dem Producte aller gegebenen Zahlen übereinstimmen; denn offenbar ist diese Bildung selbst eine der verschiedenen möglichen Anordnungen des Processes. So ist z. B.

$$abcde = (ab)c(de) = (abcd)e = (abe)(cd).$$

Es ist nicht schwierig, dieselben Sätze auch für den Fall zu beweisen, dass unter den Factoren eines Productes beliebig viele negative sind; das Vorzeichen des Productes wird das positive oder negative sein, je nachdem die Anzahl der negativen Factoren gerade oder ungerade ist.

§. 3.

Wenn die Zahl*) a das Product aus der Zahl b und einer zweiten ganzen Zahl m, also $a = mb$ ist, so nennt man a ein *Vielfaches* oder *Multiplum* von b; statt dessen sagt man auch: a ist *theilbar* durch b, oder: b ist ein *Theiler* oder *Divisor* von a, oder endlich: *b geht in a auf*. Alle diese Benennungen sind

*) Unter Zahlen schlechthin sind hier und im Folgenden immer *ganze* Zahlen zu verstehen.

gleich gebräuchlich, und da es in der Zahlentheorie ausserordentlich oft vorkommt, diese Beziehung zwischen zwei Zahlen auszudrücken, so ist es angenehm, dafür eine Reihe verschiedener Ausdrücke zu besitzen. Aus der Definition des Vielfachen leuchten nun sogleich folgende Sätze ein, von denen später sehr häufig Gebrauch gemacht werden wird.

1) Ist a Multiplum von b, b wieder Multiplum von c, so ist auch a Multiplum von c. Denn der Annahme nach ist $a = mb$, $b = nc$, wo m und n irgend zwei ganze Zahlen bedeuten; hieraus folgt $a = m(nc) = (mn)c$, also ist a theilbar durch c.

Allgemein: hat man eine Reihe von Zahlen, in welcher jede ein Vielfaches der nächstfolgenden ist, so ist auch jede frühere Zahl ein Vielfaches von jeder späteren.

2) Ist die Zahl a sowohl als auch b ein Multiplum einer dritten Zahl c, so ist auch die Summe und die Differenz der beiden ersteren ein Multiplum der dritten. Denn aus $a = mc$, $b = nc$ folgt $a \pm b = (m \pm n)\, c$.

§. 4.

Von der grössten Wichtigkeit für die Lehre von der Theilbarkeit der Zahlen ist folgende Aufgabe: Wenn irgend zwei ganze positive Zahlen a, b gegeben sind, die gemeinschaftlichen Theiler derselben, d. h. diejenigen Zahlen δ zu finden, welche gleichzeitig in a und in b aufgehen.

Wir können annehmen, es sei a grösser oder wenigstens nicht kleiner als b; dann wird die Division von a durch b einen Quotienten m und einen Rest c geben, welcher letztere jedenfalls kleiner als b ist. Betrachten wir nun die aus dieser Division resultirende Gleichung

$$a = mb + c$$

und nehmen wir an, es sei δ irgend eine sowohl in a als in b aufgehende Zahl, so ist δ jedenfalls auch ein Divisor des Restes c; denn da a und b, also auch mb Multipla von δ sind, so ist auch die Differenz $a - mb = c$ ein Multiplum von δ. Wir können daher sagen: jeder gemeinschaftliche Theiler der beiden Zahlen a, b ist auch ein gemeinschaftlicher Theiler der beiden Zahlen b, c. Umgekehrt, ist δ ein gemeinschaftlicher Divisor der beiden Zahlen b, c, so ist, da δ dann auch in mb aufgeht, die Summe $mb + c$

$= a$ der beiden Multipla mb und c von δ ebenfalls ein Multiplum von δ; also ist jeder gemeinschaftliche Divisor der Zahlen b, c auch gemeinschaftlicher Divisor der Zahlen a, b. Mithin stimmen die gemeinschaftlichen Divisoren der beiden Zahlen a, b vollständig mit denen der beiden Zahlen b, c überein; unsere Untersuchung ist daher von dem Paare a, b auf das Paar b, c reducirt, und da b nicht grösser als a, c aber jedenfalls kleiner als b ist, so können wir mit Recht sagen, dass das Problem auf ein einfacheres zurückgeführt sei.

Wenn nun c von Null verschieden ist, die erste Division also nicht aufgeht, so können wir, indem wir b durch die kleinere Zahl c dividiren, wieder eine Gleichung von der Form

$$b = nc + d$$

bilden, in welcher der Divisionsrest d kleiner als der vorhergehende c ist. Durch eine der obigen ganz ähnliche Betrachtung ergiebt sich dann, dass die gemeinschaftlichen Divisoren der beiden Zahlen c, d vollständig mit denen der Zahlen b, c und also auch mit denen der Zahlen a, b übereinstimmen.

So kann man fortfahren, bis einmal die Division aufgeht, was nach einer endlichen Anzahl von Operationen durchaus eintreten muss; denn die Zahlen $b, c, d \ldots$ bilden eine Reihe von beständig abnehmenden Zahlen, und da es nur eine endliche Anzahl von Zahlen giebt, welche kleiner sind als b, so muss unter ihnen endlich auch die Null erscheinen. Wir haben dann eine Kette von Gleichungen von der Form

$$\begin{aligned} a &= mb + c \\ b &= nc + d \\ c &= pd + e \\ &\cdots\cdots\cdots \\ &\cdots\cdots\cdots \\ f &= sg + h \\ g &= th. \end{aligned}$$

Jeder gemeinschaftliche Divisor δ von a, b ist auch Divisor der folgenden Zahlen $c, d \ldots$, endlich auch von h; umgekehrt, ist δ ein Divisor von h, so lehrt die letzte Gleichung, dass δ auch Divisor von g, also gemeinschaftlicher Divisor von g und h ist; folglich ist δ auch Divisor von f und ebenso von den vorhergehenden Zahlen, endlich auch von b und von a. Wir haben daher das Resultat:

Die gemeinschaftlichen Divisoren zweier Zahlen a und b stimmen überein mit den sämmtlichen Divisoren *einer* bestimmten Zahl h, welche man durch den obigen Algorithmus stets finden kann. Da nun h selbst zu diesen Divisoren gehört und unter ihnen dem Werth nach der grösste ist, so nennt man diese Zahl h den *grössten gemeinschaftlichen Divisor* der beiden Zahlen a und b.

Hiermit ist nun zwar unser Problem nicht vollständig gelöst, sondern nur auf das andere zurückgeführt, sämmtliche Divisoren einer gegebenen Zahl h zu finden, für welches wir noch keine directe Lösung haben; allein es wird sich im Folgenden hinreichend zeigen, dass der obige Algorithmus ein Fundament bildet, auf welchem sich die Grundprincipien der Zahlentheorie mit ebenso grosser Strenge wie Leichtigkeit aufbauen lassen. Nur eine Bemerkung noch, um auch nicht den geringsten Zweifel gegen die Allgemeinheit der folgenden Sätze aufkommen zu lassen: wir haben die obige Kette von Gleichungen gebildet unter der Voraussetzung, dass a nicht kleiner als b sei; allein für den Fall, dass $a < b$ sein sollte, braucht man nur $m = 0$, also $c = a$ zu nehmen, um dieselbe Form auch dann zu wahren.

§. 5.

Besonders interessant ist der specielle Fall, in welchem der grösste gemeinschaftliche Divisor zweier Zahlen die Einheit ist; man nennt zwei solche Zahlen *relative Primzahlen*, auch wohl *Zahlen ohne gemeinschaftlichen Divisor*, indem man absieht von dem allen Zahlen gemeinschaftlichen Divisor 1. Dieser Definition zufolge erkennt man also zwei Zahlen als relative Primzahlen daran, dass bei dem Algorithmus des grössten gemeinschaftlichen Divisors einmal der Rest $h = 1$ auftritt. Für solche Zahlen gilt nun der folgende

Hauptsatz: Sind a, b relative Primzahlen gegen einander, und ist k eine ganz beliebige dritte Zahl, so ist jeder gemeinschaftliche Theiler der beiden Zahlen ak, b auch gemeinschaftlicher Theiler der beiden Zahlen k, b.

Um sich hiervon zu überzeugen, braucht man nur sämmtliche Gleichungen, die bei dem Algorithmus des grössten gemeinschaftlichen Divisors der Zahlen a, b gebildet werden, und deren vorletzte,

da $h = 1$ ist, in unserem Falle $f = sg + 1$ lautet, mit k zu multipliciren; man erhält dann

$$\begin{aligned} ak &= mbk + ck \\ bk &= nck + dk \\ ck &= pdk + ek \\ &\cdots\cdots\cdots \\ &\cdots\cdots\cdots \\ fk &= sgk + k. \end{aligned}$$

Ist nun δ irgend ein gemeinschaftlicher Divisor von ak und b, so geht δ auch in mbk, also auch in $ak - mbk = ck$ auf; es geht daher δ auch in nck und folglich auch in $bk - nck = dk$ auf. Und indem man diese Schlussweise fortsetzt, gelangt man zu dem Resultat, dass δ auch in fk, in gk, folglich auch in $fk - sgk = k$ aufgehen muss, was zu beweisen war.

Im Folgenden werden wir vorzüglich zwei specielle Fälle dieses Satzes gebrauchen, nämlich:

1) Das Product zweier Zahlen a und k, deren jede relative Primzahl gegen eine dritte b ist, ist gleichfalls relative Primzahl gegen b; denn unserem Satze nach haben ak und b dieselben gemeinschaftlichen Divisoren, wie k und b; da aber k und b relative Primzahlen sind, so haben sie nur den einzigen gemeinschaftlichen Divisor 1; dasselbe gilt daher von ak und b, also sind diese beiden Zahlen relative Primzahlen.

2) Sind a und b relative Primzahlen zu einander, und ist ak durch b theilbar, so ist auch k durch b theilbar; denn da der Annahme zufolge ak und b den gemeinschaftlichen Divisor b haben, so muss dem Hauptsatze nach b auch gemeinschaftlicher Divisor von k und b, also jedenfalls Divisor von k sein.

3) Den ersten dieser beiden Sätze kann man leicht verallgemeinern. Ist jede der Zahlen $a, b, c, d \ldots$ relative Primzahl gegen eine Zahl α, so ist auch ab, folglich auch das Product abc aus ab und c, folglich auch das Product $abcd$ aus abc und d, u. s. f. kurz das Product $abcd \ldots$ aller jener Zahlen ebenfalls relative Primzahl gegen α. Allgemeiner, hat man zwei Reihen von Zahlen

$$a, \; b, \; c, \; d \; \ldots$$

und

$$\alpha, \; \beta, \; \gamma \; \ldots$$

von der Beschaffenheit, dass jede Zahl der einen Reihe relative

Primzahl gegen jede Zahl der andern Reihe ist, so ist auch das Product $abcd\ldots$ aller Zahlen der einen Reihe relative Primzahl gegen das Product $\alpha\beta\gamma\ldots$ aller Zahlen der andern Reihe. Denn soeben ist bewiesen, dass jede der Zahlen $\alpha, \beta, \gamma\ldots$ relative Primzahl gegen das Product $abcd\ldots$ ist, woraus durch nochmalige Anwendung desselben Satzes auch folgt, dass ihr Product $\alpha\beta\gamma\ldots$ ebenfalls relative Primzahl gegen $abcd\ldots$ ist.

4) Hieraus können wir wieder einen speciellen Fall ableiten, indem wir annehmen, dass die Zahlen $b, c, d\ldots$ identisch mit a, ferner die Zahlen $\beta, \gamma\ldots$ identisch mit α sind; wir erhalten dann das Resultat: ist a relative Primzahl gegen α, so ist auch jede Potenz der Zahl a relative Primzahl gegen jede Potenz der Zahl α.

Eine Anwendung findet dieser Satz bei dem Beweise, dass $\sqrt[m]{A}$ irrational ist, wenn die ganze Zahl A nicht die $m$te Potenz einer ganzen Zahl ist. Wäre nämlich $\sqrt[m]{A}$ rational, also von der Form $\frac{r}{s}$, wo r und s zwei ganze Zahlen sind, die man ohne gemeinschaftlichen Divisor annehmen kann, so wäre $\left(\frac{r}{s}\right)^m = \frac{r^m}{s^m} = A$, also r^m theilbar durch s^m, obgleich r^m und s^m relative Primzahlen sind; dies wäre eben nur dann möglich, wenn $s^m = 1$, also auch $s = 1$, und folglich $A = r^m$ die $m$te Potenz einer ganzen Zahl r wäre.

§. 6.

Die Aufgabe des §. 4 in der Weise verallgemeinert, dass für eine ganze Reihe gegebener Zahlen $a, b, c, d\ldots$ alle gemeinschaftlichen Divisoren gesucht werden, führt zu einem ganz ähnlichen Resultate. Es sei h der grösste gemeinschaftliche Divisor von a und b, so ist, wie wir früher fanden, jeder gemeinschaftliche Divisor von a und b auch Divisor von h und umgekehrt; jeder gemeinschaftliche Divisor der drei Zahlen a, b, c ist daher auch gemeinschaftlicher Divisor von h, c und umgekehrt; bezeichnet man daher mit k den grössten gemeinschaftlichen Divisor von h und c, so ist jede gleichzeitig in a, b, c aufgehende Zahl Divisor von k, und umgekehrt wird jeder Divisor von k auch Divisor der drei Zahlen a, b, c sein. Bildet man ferner den grössten gemeinschaft-

lichen Divisor l der beiden Zahlen k und d, so stimmen die gemeinschaftlichen Divisoren der vier Zahlen a, b, c, d vollständig überein mit den sämmtlichen Divisoren der Zahl l u. s. f. Wir haben daher das Resultat: ist irgend eine Reihe von Zahlen $a, b, c, d \ldots$ gegeben, so giebt es stets eine — und natürlich auch nur eine — Zahl m von der Beschaffenheit, dass jede gleichzeitig in a, in b, in c, in d u. s. w. aufgehende Zahl auch in m aufgeht, und umgekehrt jeder Divisor von m auch Divisor jeder einzelnen der Zahlen $a, b, c, d \ldots$ ist. Diese vollkommen bestimmte Zahl m heisst deshalb wieder der *grösste gemeinschaftliche Divisor* der gegebenen Zahlen.

§. 7.

Gewissermaassen das Umgekehrte der vorhergehenden ist die folgende Aufgabe: Wenn eine Reihe von Zahlen $a, b, c, d \ldots$ gegeben ist, alle gemeinschaftlichen Multipla derselben, d. h. alle Zahlen zu finden, welche durch jede einzelne der gegebenen Zahlen theilbar sind. Da von den gesuchten Zahlen zuerst gefordert wird, dass sie durch a theilbar sein sollen, so sind sie jedenfalls in der Form sa enthalten, wo s irgend eine ganze Zahl bedeutet. Ist nun δ der grösste gemeinschaftliche Divisor der beiden Zahlen a und b, so sind offenbar $\frac{a}{\delta}$ und $\frac{b}{\delta}$ relative Primzahlen; soll daher $sa = s\frac{a}{\delta} \cdot \delta$ theilbar sein durch $b = \frac{b}{\delta} \cdot \delta$, so muss $s\frac{a}{\delta}$ durch $\frac{b}{\delta}$, und folglich [§. 5, 2)] auch s durch $\frac{b}{\delta}$ theilbar, also von der Form $s'\frac{b}{\delta}$ sein, wo s' wieder irgend eine ganze Zahl bedeutet. Sämmtliche sowohl durch a, als durch b theilbare Zahlen sind daher von der Form $sa = s'\frac{ab}{\delta}$; und umgekehrt leuchtet ein, dass alle in dieser Form enthaltenen Zahlen sowohl durch a als durch b theilbar sind; denn es ist ja

$$s'\frac{ab}{\delta} = s'\frac{b}{\delta} \cdot a = s'\frac{a}{\delta} \cdot b.$$

Es zeigt sich also, dass die sämmtlichen gemeinschaftlichen Multipla der beiden Zahlen a, b übereinstimmen mit den sämmtlichen

Vielfachen *einer* bestimmten Zahl $\frac{ab}{\delta}$, welche man deshalb das *kleinste gemeinschaftliche Vielfache* der beiden Zahlen a, b nennt.

Um diesen Satz für eine beliebige Anzahl gegebener Zahlen $a, b, c, d \dots$ zu verallgemeinern, braucht man nur zu bemerken, dass jedes gemeinschaftliche Vielfache der Zahlen

$$a, \ b, \ c, \ d \ \dots$$

nothwendig auch ein gemeinschaftliches Vielfaches der Zahlen

$$\frac{ab}{\delta}, \ c, \ d \ \dots$$

ist und umgekehrt. Man wird daher zunächst das kleinste gemeinschaftliche Multiplum $\varkappa$ der beiden Zahlen $\frac{ab}{\delta}$ und c suchen, dann das kleinste gemeinschaftliche Vielfache λ von $\varkappa$ und d u. s. f. Auf diese Weise leuchtet ein, dass sämmtliche gemeinschaftliche Multipla der gegebenen Zahlen $a, b, c, d \dots$ übereinstimmen mit den sämmtlichen Vielfachen einer einzigen vollständig bestimmten Zahl μ, welche man deshalb das *kleinste gemeinschaftliche Vielfache* der gegebenen Zahlen nennt.

Von besonderer Wichtigkeit ist noch der Fall, in welchem die sämmtlichen gegebenen Zahlen $a, b, c, d \dots$ relative Primzahlen gegen einander sind, so dass je zwei unter ihnen ausser der Einheit keinen gemeinschaftlichen Divisor haben. In diesem Fall ist zunächst $\delta = 1$, also ist das kleinste gemeinschaftliche Vielfache der beiden relativen Primzahlen a und b ihr Product ab. Da nun c wieder relative Primzahl gegen a und gegen b, also [§. 5, 1)] auch gegen ab ist, so ist abc das kleinste gemeinschaftliche Multiplum der drei Zahlen a, b, c u. s. f. Kurz, man erhält das Resultat: Sind $a, b, c, d \dots$ relative Primzahlen unter einander, so ist jede Zahl, welche durch jede einzelne derselben theilbar ist, auch durch ihr Product $abcd \dots$ theilbar.

§. 8.

Da jede Zahl sowohl durch die Einheit, als auch durch sich selbst theilbar ist, so hat jede Zahl — die Einheit selbst ausgenommen — mindestens zwei Divisoren. Jede Zahl nun, welche keine anderen als diese beiden Divisoren besitzt, heisst eine *Prim-*

zahl (numerus primus); es ist zweckmässig, die Einheit nicht zu den Primzahlen zu rechnen, weil manche Sätze über Primzahlen nicht für die Zahl 1 gültig bleiben.

Aus dieser Erklärung leuchtet sogleich ein, dass, wenn p eine Primzahl und a irgend eine ganze Zahl ist, immer einer von den beiden folgenden einander ausschliessenden Fällen Statt finden muss: entweder geht p in a auf, oder p ist relative Primzahl gegen a; denn der grösste gemeinschaftliche Divisor von p und a ist entweder p selbst oder die Einheit.

Hieraus folgt weiter: Wenn ein Product aus mehreren Zahlen $a, b, c, d \ldots$ durch eine Primzahl p theilbar ist, so geht p mindestens in einem der Factoren $a, b, c, d \ldots$ auf. Denn wäre keine einzige dieser Zahlen durch p theilbar, so wäre p relative Primzahl gegen jede einzelne von ihnen und folglich auch gegen ihr Product, was gegen die Annahme streitet, dass dies Product durch p theilbar ist.

Jede Zahl, welche ausser sich selbst und der Einheit noch andere Divisoren hat, heisst *zusammengesetzt (numerus compositus)*. Diese Benennung wird gerechtfertigt durch folgenden

Fundamentalsatz: Jede zusammengesetzte Zahl lässt sich stets und nur auf eine einzige Weise als Product aus einer endlichen Anzahl von Primzahlen darstellen.

Beweis. Da jede zusammengesetzte Zahl m ausser 1 und m noch andere Divisoren hat, so sei a ein solcher; ist nun a keine Primzahl, also eine zusammengesetzte Zahl, so besitzt a ausser 1 und a noch andere Divisoren, z. B. b; ist b noch keine Primzahl, also zusammengesetzt, so hat b wieder mindestens einen Divisor c, der von 1 und b verschieden ist. Fährt man so fort, so muss man endlich einmal zu einer Primzahl gelangen; denn die Reihe der Zahlen $m, a, b, c \ldots$ ist eine abnehmende, sie kann also, da es nur eine endliche Anzahl von Zahlen giebt, welche kleiner als m sind, nur eine endliche Anzahl von Gliedern enthalten; das letzte Glied derselben muss aber eine Primzahl sein, denn sonst könnte man ja die Reihe noch weiter fortsetzen. Bezeichnet man diese Primzahl mit p, so ist, da jedes Glied der Reihe ein Multiplum des folgenden ist, die erste Zahl m auch ein Multiplum von der letzten p. Man kann daher

$$m = pm'$$

setzen. Nun ist m' entweder eine Primzahl — dann ist m schon

als Product von Primzahlen dargestellt — oder m' ist zusammengesetzt; im letzteren Fall muss es wieder eine in m' aufgehende Primzahl p' geben, so dass

$$m' = p'm'', \text{ also } m = pp'm''$$

wird. Ist nun m'' noch keine Primzahl, so kann man auf dieselbe Weise fortfahren, bis man m als Product von lauter Primzahlen dargestellt hat. Dass dies wirklich nach einer endlichen Anzahl von ähnlichen Zerlegungen geschehen muss, leuchtet daraus ein, dass die Reihe der Zahlen $m, m', m'' \ldots$ ebenfalls eine abnehmende und folglich eine endliche ist.

Hiermit ist der eine Hauptttheil des Satzes erwiesen, welcher die Möglichkeit der Zerlegung behauptet; offenbar ist aber diese successive Ablösung von Primzahl-Factoren in mancher Beziehung willkürlich, und es bleibt daher noch nachzuweisen übrig, dass, auf welche Weise dieselbe auch ausgeführt sein mag, das Endresultat doch stets dasselbe sein muss. Nehmen wir daher an, man habe durch zwei verschiedene Anordnungen einmal

$$m = pp'p'' \ldots$$

ein anderes Mal

$$m = qq'q'' \ldots$$

gefunden, wo $p, p', p'' \ldots$ und $q, q', q'' \ldots$ sämmtlich Primzahlen bedeuten. Da nun das Product $pp'p'' \ldots$ durch die Primzahl q theilbar ist, so muss mindestens einer der Factoren, z. B. p, durch q theilbar sein; p besitzt aber als Primzahl nur die beiden Divisoren 1 und p, und folglich muss $q = p$ sein, da q nicht $= 1$ ist. Hieraus folgt nun

$$p'p'' \ldots = q'q'' \ldots$$

und man kann auf dieselbe Weise zeigen, dass q' mit einer der Primzahlen $p', p'' \ldots$, z. B. mit p', identisch sein muss, woraus dann wieder

$$p'' \ldots = q'' \ldots$$

folgt. Auf diese Weise überzeugt man sich davon, dass jede Primzahl, welche bei der zweiten Art der Zerlegung ein oder mehrere Male als Factor auftritt, mindestens ebenso oft auch bei der ersten Zerlegung vorkommt; da aber ferner auf dieselbe Weise gezeigt werden kann, dass sie bei der zweiten Zerlegung mindestens ebenso oft vorkommt wie bei der ersten, so muss jede

Primzahl in beiden Zerlegungen gleich oft als Factor vorkommen, und folglich stimmt der Complex aller Primzahlen bei der einen Zerlegung vollständig mit dem bei der andern überein.

Nachdem so der Satz in allen seinen Theilen bewiesen ist, können wir die Darstellung der zusammengesetzten Zahl m noch dadurch vereinfachen, dass wir jedesmal alle unter einander identischen Primzahl-Factoren zu einer Potenz vereinigen. Es sei nämlich a eine von den in m aufgehenden Primzahlen, und zwar mag dieselbe genau α mal als Factor in der Zerlegung vorkommen, so vereinigen wir diese α Factoren zu der Potenz a^α; sind hierdurch noch nicht alle Factoren erschöpft, und ist b eine der übrigen Primzahlen, so bilden wir, wenn sie genau β mal vorkommt, die Potenz b^β, und in derselben Weise fahren wir fort, wenn hierdurch noch nicht alle Primzahlfactoren von m erschöpft sind. Auf diese Weise überzeugt man sich, dass man jeder zusammengesetzten Zahl m die Form

$$m = a^\alpha b^\beta c^\gamma \ldots$$

geben kann, in welcher $a, b, c \ldots$ die sämmtlichen unter einander verschiedenen, in m aufgehenden Primzahlen, und $\alpha, \beta, \gamma \ldots$ ganze positive Zahlen bedeuten. Dass aber in dieser Form nicht nur alle zusammengesetzten, sondern auch alle Primzahlen enthalten sind, leuchtet unmittelbar ein.

Die Primzahlen bilden daher gewissermaassen das Material, aus welchem alle anderen Zahlen sich zusammensetzen lassen. Dass es eine unbegrenzte Anzahl solcher Primzahlen giebt, hat schon *Euclid* bewiesen, und zwar in folgender Art. Gesetzt es gäbe nur eine endliche Anzahl von Primzahlen, so würde eine von ihnen, die wir mit p bezeichnen wollen, die letzte, d. h. die grösste sein. Denken wir uns nun alle diese Primzahlen aufgeschrieben

$$2, 3, 5, 7, 11 \ldots p,$$

so müsste jede Zahl, welche grösser als p ist, zusammengesetzt und folglich durch mindestens eine dieser Primzahlen theilbar sein. Allein es ist sehr leicht, eine Zahl zu bilden, welche erstens grösser als p und zweitens durch keine jener Primzahlen theilbar ist; dazu bilden wir das Product aller Primzahlen von 2 bis p und vergrössern dasselbe um eine Einheit. Diese Zahl

$$z = 2.\ 3.\ 5 \ldots p + 1$$

ist in der That grösser als p, da ja schon $2p$ grösser als p ist; sie ist aber durch keine der Primzahlen theilbar, da ja z, durch jede derselben dividirt, immer den Rest 1 lässt. Damit ist also unsere Annahme im Widerspruch, und folglich giebt es unendlich viele Primzahlen.

Dieser Satz ist nur ein specieller Fall des andern, dass in jeder unbegrenzten arithmetischen Progression, deren allgemeines Glied $kx + m$ ist, und in welcher das Anfangsglied m und die Differenz k relative Primzahlen sind, unendlich viele Primzahlen enthalten sind; allein, so einfach der Beweis für den speciellen Fall war, in welchem $k = 1$, so schwierig war es, einen strengen Beweis für den allgemeinen Satz zu geben, und dies ist bis jetzt nur durch Zuziehung von Principien gelungen, welche der Infinitesimalrechnung angehören *).

§. 9.

Durch den soeben bewiesenen Fundamentalsatz haben wir nun ein einfaches Kriterium gewonnen, nach welchem stets beurtheilt werden kann, ob eine Zahl m durch eine andere n theilbar ist oder nicht, sobald wir voraussetzen dürfen, dass beide in ihre Primfactoren zerlegt sind. Nehmen wir nämlich an, dass m durch n theilbar, dass also $m = nq$ ist, so leuchtet ein, dass jede in n aufgehende Primzahl auch in m aufgehen muss; es kann daher n keine andern Primfactoren enthalten als m, und ausserdem kann auch ein solcher Primfactor nicht öfter in n als in m vorkommen; und umgekehrt, wenn jeder Primfactor der Zahl n mindestens ebenso oft in m vorkommt wie in n, so ist auch m durch n theilbar.

Sind daher $a, b, c \dots$ die sämmtlichen von einander verschiedenen, in m aufgehenden Primzahlen, so dass

$$m = a^\alpha b^\beta c^\gamma \dots$$

so ist jeder Divisor n dieser Zahl in der Form

$$n = a^{\alpha'} b^{\beta'} c^{\gamma'} \dots$$

enthalten, in welcher

*) Siehe die Supplemente VI. §. 132—137.

α' irgend eine der $\alpha + 1$ Zahlen $0, 1, 2 \ldots \alpha$
β' „ „ „ $\beta + 1$ „ $0, 1, 2 \ldots \beta$
γ' „ „ „ $\gamma + 1$ „ $0, 1, 2 \ldots \gamma$
u. s. w.

bedeutet; und alle diese Zahlen n sind wirklich Divisoren von m. Hieraus gehen sogleich einige interessante Folgerungen hervor.

Zunächst leuchtet ein, da jede Combination eines Werthes von α' mit einem von β', mit einem von γ' u. s. w. einen Divisor von m liefert, und da je zwei verschiedenen solchen Combinationen (nach §. 8) auch zwei ungleiche Divisoren von m entsprechen, dass die Anzahl aller Divisoren von m gleich

$$(\alpha + 1)(\beta + 1)(\gamma + 1) \cdots$$

ist; diese Anzahl hängt daher nur von den Exponenten $\alpha, \beta, \gamma \ldots$ ab, nicht aber von der Natur der in m aufgehenden Primzahlen a, b, c u. s. w.

Bildet man ferner das Schema

$$\begin{array}{l} 1, a, a^2 \ldots a^\alpha \\ 1, b, b^2 \ldots b^\beta \\ 1, c, c^2 \ldots c^\gamma \\ \text{u. s. w.} \end{array}$$

und bildet alle Producte $a^{\alpha'} b^{\beta'} c^{\gamma'} \cdots$, indem man aus jeder dieser Horizontalreihen ein Glied $a^{\alpha'}, b^{\beta'}, c^{\gamma'} \ldots$ auswählt, so erhält man alle Divisoren der Zahl m, und zwar jeden nur ein einziges Mal. Die Summe aller dieser Divisoren erhält man daher nach derselben Regel, nach welcher man die einzelnen Aggregate

$$1 + a + a^2 + \cdots + a^\alpha = \frac{a^{\alpha+1} - 1}{a - 1}$$

$$1 + b + b^2 + \cdots + b^\beta = \frac{b^{\beta+1} - 1}{b - 1}$$

$$1 + c + c^2 + \cdots + c^\gamma = \frac{c^{\gamma+1} - 1}{c - 1}$$

u. s. w.

mit einander zu multipliciren hat; folglich ist die Summe aller Divisoren der Zahl m gleich dem Product

$$\frac{a^{\alpha+1} - 1}{a - 1} \cdot \frac{b^{\beta+1} - 1}{b - 1} \cdot \frac{c^{\gamma+1} - 1}{c - 1} \cdots$$

Nehmen wir z. B. $m = 60 = 2^2.3.5$, so sind die sämmtlichen Divisoren folgende:

$$1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60;$$

ihre Anzahl ist

$$(2+1)(1+1)(1+1) = 12$$

und ihre Summe

$$\frac{2^3-1}{2-1} \cdot \frac{3^2-1}{3-1} \cdot \frac{5^2-1}{5-1} = 7 \cdot 4 \cdot 6 = 168.$$

§. 10.

Wir kehren nun zu einigen früheren Aufgaben zurück, zunächst zu derjenigen (§. 6), den grössten gemeinschaftlichen Divisor einer Reihe von Zahlen zu bilden, deren Zerlegungen in Primfactoren gegeben sind. Man betrachte alle Primzahlen, welche in diesen Zerlegungen vorkommen, und scheide zunächst diejenigen unter ihnen aus, welche in einer oder mehreren der gegebenen Zahlen gar nicht als Primfactoren enthalten sind. Bleibt auf diese Weise gar keine Primzahl übrig, so ist die Einheit der gesuchte grösste gemeinschaftliche Divisor. Im entgegengesetzten Fall sei a eine Primzahl, welche bei dieser vorläufigen Ausscheidung zurückgeblieben ist und also in jeder der gegebenen Zahlen mindestens einmal enthalten ist; man zähle, wie oft a als Primfactor in jeder einzelnen der gegebenen Zahlen vorkommt, und nehme die kleinste dieser Anzahlen, die wir mit α bezeichnen, so dass a in mindestens einer der gegebenen Zahlen genau α mal, in allen übrigen aber mindestens ebenso oft als Primfactor vorkommt. Aehnlich verfahre man mit den übrigen Primzahlen $b, c \ldots$, sofern diese noch nicht erschöpft sind, und bilde für jede, für b die Anzahl β, für c die Anzahl γ u. s. w. nach derselben Regel, nach welcher für die Primzahl a die Anzahl α gebildet wurde. Dann ist

$$a^\alpha \, b^\beta \, c^\gamma \ldots$$

der gesuchte grösste gemeinschaftliche Divisor. Der Beweis für diese Regel leuchtet unmittelbar dadurch ein, dass der grösste gemeinschaftliche Divisor keine anderen Primfactoren enthalten kann, als solche, welche in jeder der gegebenen Zahlen enthalten

sind, und dass er keinen Primfactor öfter enthalten kann, als irgend eine der gegebenen Zahlen.

Aehnlich gestaltet sich die Lösung der anderen Aufgabe, das kleinste gemeinschaftliche Multiplum einer Reihe von gegebenen Zahlen zu bilden (§. 7). Jetzt betrachte man *jede* Primzahl, die in irgend einer der gegebenen Zahlen als Factor enthalten ist, und sehe nach, in welcher sie am häufigsten vorkommt; ebenso oft nehme man sie als Factor in das kleinste gemeinschaftliche Multiplum auf; sind daher $a, b, c \ldots$ die sämmtlichen Primzahlen, welche in den einzelnen Zerlegungen der gegebenen Zahlen vorkommen, so erhält man nach dieser Regel das gesuchte kleinste gemeinschaftliche Multiplum in der Form

$$a^{\alpha'} b^{\beta'} c^{\gamma'} \ldots,$$

wo z. B. der Exponent α' dadurch bestimmt ist, dass die Primzahl a in mindestens einer der gegebenen Zahlen genau α' mal, in allen übrigen aber nicht öfter als Factor enthalten ist. Der Beweis liegt hier darin, dass die gesuchte Zahl jeden Primfactor enthalten muss, der in einer der gegebenen Zahlen enthalten ist, und zwar mindestens ebenso oft, als diese.

Endlich können wir aus den vorhergehenden Principien noch ein Kriterium ableiten, nach welchem zu erkennen ist, ob eine Zahl

$$m = a^{\alpha} b^{\beta} c^{\gamma} \ldots$$

eine genaue $r$te Potenz einer ganzen Zahl k ist. Dazu ist offenbar erforderlich und hinreichend, dass alle Exponenten $\alpha, \beta, \gamma \ldots$ durch r theilbar sind, wie man sogleich aus der Annahme

$$m = k^r$$

erkennt.

§. 11.

Wir gehen nun zu einer Untersuchung über, welche an sich schon interessant und ausserdem für die Folge von der grössten Wichtigkeit ist. Denken wir uns einmal alle ganzen Zahlen

$$1, 2, 3, 4 \ldots m$$

bis zu einer beliebigen letzten m aufgeschrieben, und zählen wir ab, wie viele von ihnen relative Primzahlen gegen die letzte m sind. Diese Anzahl bezeichnet man in der Zahlentheorie durch-

gängig mit $\varphi(m)$, wo der Buchstabe φ die Rolle eines Functionszeichens spielt. Da die Einheit relative Primzahl gegen sich selbst ist, so folgt zunächst

$$\varphi(1) = 1;$$

durch wirkliches Abzählen findet man ferner

$$\varphi(2) = 1, \quad \varphi(3) = 2, \quad \varphi(4) = 2, \quad \varphi(5) = 4$$

u. s. w. Allein es kommt darauf an, einen allgemeinen Ausdruck für die Function $\varphi(m)$ zu finden, und wir werden sehen, dass man zu diesem Zweck nur die sämmtlichen von einander verschiedenen Primzahlen $a, b, c \ldots$ zu kennen braucht, welche in m aufgehen. Unsere Aufgabe ist nämlich identisch mit dieser: die Anzahl der obigen Zahlen zu bestimmen, welche durch keine dieser Primzahlen $a, b, c \ldots$ theilbar sind; und diese ist wieder nur ein specieller Fall der folgenden:

Wenn $a, b, c \ldots$ relative Primzahlen unter einander sind (d. h. immer, dass jede der Zahlen $a, b, c \ldots$ relative Primzahl ist gegen alle übrigen) und sämmtlich in einer Zahl m aufgehen; so soll die Anzahl derjenigen der Zahlen

$$1, 2, 3 \ldots m \qquad (M)$$

bestimmt werden, welche durch keine der Zahlen $a, b, c \ldots$ theilbar sind.

Es zeigt sich nun, wie es häufig geschieht, dass die allgemeinere Aufgabe leichter zu lösen ist, als der direct angegriffene specielle Fall. Zu diesem Zweck scheiden wir zunächst aus dem Zahlencomplex (M) alle diejenigen aus, welche durch die Zahl a theilbar sind; es sind dies offenbar die Zahlen

$$a, \; 2a, \; 3a \cdots \frac{m}{a} a;$$

die Anzahl derselben ist $\frac{m}{a}$; es bleiben daher, nachdem dieselben aus dem Complex (M) ausgeschieden sind, nur

$$m - \frac{m}{a} = m\left(1 - \frac{1}{a}\right) \qquad (1)$$

Zahlen übrig, welche nicht durch a theilbar sind, und deren Complex wir mit (A) bezeichnen wollen.

Aus diesem Complex (A) sind nun zunächst alle durch b theilbaren Zahlen auszuscheiden; es sind dies offenbar alle diejenigen Zahlen des Complexes (M), welche der doppelten Forderung ge-

nügen, erstens dass sie nicht durch a, zweitens dass sie durch b theilbar sind. Alle Zahlen nun, welche der zweiten Forderung genügen, sind die folgenden

$$b,\ 2b,\ 3b, \cdots \frac{m}{b}\,b;$$

damit aber eine dieser Zahlen, z. B. rb, auch der ersten Forderung genüge, ist erforderlich und hinreichend, dass der Coefficient r nicht durch a theilbar sei; denn da der Annahme nach a und b relative Primzahlen sind, so ist rb theilbar oder nicht theilbar durch a, je nachdem r durch a theilbar ist oder nicht [§. 5, 2)]. Die Anzahl der noch aus dem Complex (A) auszuscheidenden Zahlen stimmt daher überein mit der Anzahl derjenigen der Zahlen

$$1, 2, 3 \cdots \frac{m}{b},$$

welche nicht durch a theilbar sind. Da nun m durch a und b, folglich auch durch ab theilbar ist, so ist die letzte dieser Zahlen $\frac{m}{b}$ theilbar durch a; unsere Frage ist also dieselbe für die Zahl $\frac{m}{b}$ wie diejenige, welche wir durch den ersten Schritt für die Zahl m gelöst und durch die Formel (1) beantwortet haben. Die Anzahl der aus (A) auszuscheidenden Zahlen ist daher gleich

$$\frac{m}{b}\left(1-\frac{1}{a}\right)$$

und wir erhalten

$$m\left(1-\frac{1}{a}\right)-\frac{m}{b}\left(1-\frac{1}{a}\right)=m\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right) \qquad (2)$$

als Anzahl derjenigen im Complex (A) enthaltenen Zahlen, welche nicht durch b theilbar sind, oder, was dasselbe ist, als Anzahl derjenigen in (M) enthaltenen Zahlen, welche weder durch a noch durch b theilbar sind.

Bezeichnen wir den Complex dieser Zahlen mit (B), so kann man in derselben Weise fortfahren und gelangt so durch Induction zu dem Resultat, dass die Anzahl derjenigen in (M) enthaltenen Zahlen (K), welche durch keine der Zahlen $a, b, c \ldots k$ theilbar sind, gleich

$$m\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)\left(1-\frac{1}{c}\right)\cdots\left(1-\frac{1}{k}\right) \qquad (3)$$

ist. Um die Allgemeingültigkeit dieses Gesetzes nachzuweisen,

nehmen wir an, dass die Richtigkeit desselben für die Zahlen $a, b, c \dots k$ schon bewiesen sei, und untersuchen, was geschieht, wenn zu denselben noch eine andere l hinzukommt, wobei natürlich wieder vorausgesetzt wird, erstens dass l in m aufgeht, zweitens dass l relative Primzahl gegen jede der vorhergehenden Zahlen $a, b, c \dots k$ ist.

Um die Anzahl aller in (M) enthaltenen Zahlen zu bestimmen, welche durch keine der Zahlen $a, b, c \dots k, l$ theilbar sind, haben wir aus dem Complex (K) derjenigen Zahlen, welche durch keine der Zahlen $a, b, c \dots k$ theilbar sind, und deren Anzahl durch die Formel (3) gegeben ist, nur noch die auszuscheiden, welche durch l theilbar sind; es sind dies alle diejenigen in (M) enthaltenen Zahlen, welche erstens nicht theilbar durch $a, b, c \dots k$, zweitens theilbar durch l sind. Alle durch l theilbaren Zahlen des Complexes (M) sind diese

$$l,\ 2l,\ 3l \dots \frac{m}{l} l,$$

und damit irgend eine derselben, z. B. $r\,l$, durch keine der Zahlen $a, b \dots k$ theilbar sei, ist erforderlich und hinreichend, dass der Coefficient r dieselbe Eigenschaft habe. Die Anzahl der auszuscheidenden Zahlen stimmt daher überein mit der Anzahl derjenigen unter den Zahlen

$$1,\ 2, \dots \frac{m}{l},$$

welche durch keine der Zahlen $a, b \dots k$ theilbar sind; diese ist aber nach der als richtig vorausgesetzten Formel (3) gleich

$$\frac{m}{l}\left(1 - \frac{1}{a}\right)\left(1 - \frac{1}{b}\right) \dots \left(1 - \frac{1}{k}\right);$$

nach Ausscheidung derselben aus dem Complex (K) bleiben daher

$$\begin{aligned} & m\left(1 - \frac{1}{a}\right)\left(1 - \frac{1}{b}\right) \dots \left(1 - \frac{1}{k}\right) \\ & - \frac{m}{l}\left(1 - \frac{1}{a}\right)\left(1 - \frac{1}{b}\right) \dots \left(1 - \frac{1}{k}\right) \\ & = m\left(1 - \frac{1}{a}\right)\left(1 - \frac{1}{b}\right) \dots \left(1 - \frac{1}{k}\right)\left(1 - \frac{1}{l}\right) \end{aligned}$$

Zahlen übrig, nämlich diejenigen, welche durch keine der Zahlen $a, b, c \dots k, l$ theilbar sind.

Hiermit ist die Allgemeingültigkeit unseres Satzes bewiesen; kehren wir nun zu unserer ursprünglichen Aufgabe zurück, so erhalten wir das Resultat:

Sind $a, b \ldots k, l$ die sämmtlichen von einander verschiedenen in m aufgehenden Primzahlen, so ist

$$\varphi(m) = m\left(1 - \frac{1}{a}\right)\left(1 - \frac{1}{b}\right)\cdots\left(1 - \frac{1}{k}\right)\left(1 - \frac{1}{l}\right)$$

die Anzahl aller derjenigen der Zahlen

$$1, 2 \ldots m,$$

welche relative Primzahlen gegen die letzte m sind.

Denn damit irgend eine Zahl relative Primzahl gegen m sei, ist erforderlich und hinreichend, dass sie durch keine der in m aufgehenden absoluten Primzahlen theilbar sei.

Wir können dem gefundenen Ausdruck eine andere Form geben, indem wir m als Product von Primzahl-Potenzen darstellen; da $a, b, c \ldots$ die sämmtlichen von einander verschiedenen in m aufgehenden Primzahlen sind, so hat m die Form

$$m = a^\alpha b^\beta c^\gamma \ldots$$

und es wird

$$\varphi(m) = (a-1)\,a^{\alpha-1}\cdot(b-1)\,b^{\beta-1}\cdot(c-1)\,c^{\gamma-1}\ldots$$

Um unseren Satz an einem Beispiel zu prüfen, wählen wir $m = 60$; die sämmtlichen Zahlen, welche nicht grösser als 60 und relative Primzahlen gegen 60 sind, bilden die Reihe

1, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53, 59,

und ihre Anzahl ist = 16; in der That finden wir nach der obigen Formel, da 2, 3, 5 sämmtliche in 60 aufgehende Primzahlen sind,

$$\varphi(60) = 60\cdot\frac{1}{2}\cdot\frac{2}{3}\cdot\frac{4}{5} = 16.$$

§. 12.

Aus der gefundenen Form der Function $\varphi(m)$ geht auch noch folgender Satz hervor: Sind m und m' zwei relative Primzahlen, so ist

$$\varphi(mm') = \varphi(m) \quad \varphi(m').$$

Denn sind $a, b, c \ldots$ sämmtliche in m, und $a', b', c' \ldots$ sämmtliche in m' aufgehende Primzahlen, so stimmt, da m und m' relative Primzahlen sind, keine Primzahl der einen Reihe mit einer der andern überein, d. h. alle Primzahlen

$$a, \; b, \; c \; \ldots \qquad a', \; b', \; c' \; \ldots$$

sind von einander verschieden. Sie gehen ferner sämmtlich in dem Product mm' auf, und umgekehrt muss jede in mm' aufgehende Primzahl, da sie in einem der beiden Factoren m, m' aufgehen muss, mit einer dieser Primzahlen übereinstimmen. Also sind dies die sämmtlichen von einander verschiedenen in mm' aufgehenden Primzahlen; hieraus folgt

$$\varphi(mm') = mm' \left\{ \begin{array}{l} \left(1 - \frac{1}{a}\right)\left(1 - \frac{1}{b}\right)\left(1 - \frac{1}{c}\right) \ldots \\ \left(1 - \frac{1}{a'}\right)\left(1 - \frac{1}{b'}\right)\left(1 - \frac{1}{c'}\right) \ldots \end{array} \right\}$$

Da nun andererseits

$$\varphi(m) = m \left(1 - \frac{1}{a}\right)\left(1 - \frac{1}{b}\right)\left(1 - \frac{1}{c}\right) \ldots$$

und

$$\varphi(m') = m' \left(1 - \frac{1}{a'}\right)\left(1 - \frac{1}{b'}\right)\left(1 - \frac{1}{c'}\right) \ldots$$

ist, so ergiebt sich durch den unmittelbaren Anblick die Richtigkeit des zu beweisenden Satzes.

So ist z. B.

$$\varphi(60) = \varphi(4 \cdot 15) = \varphi(4)\, \varphi(15) = 2 \cdot 8 = 16.$$

Uebrigens leuchtet ein, dass der soeben bewiesene Satz ohne Weiteres auf ein Product aus beliebig vielen Zahlen $m, m', m'' \ldots$ ausgedehnt werden kann, welche sämmtlich unter einander relative Primzahlen sind; denn es ist z. B.

$$\varphi(mm'm'') = \varphi(m)\, \varphi(m'm'') = \varphi(m)\, \varphi(m')\, \varphi(m'')$$

und ähnlich für eine grössere Anzahl von Factoren.

§. 13.

Die Aufgabe, den Werth der Function $\varphi(m)$ zu bestimmen, ist eigentlich nur ein specieller Fall von der folgenden:

Wenn δ irgend ein Divisor der Zahl m ist, die Anzahl derjenigen der Zahlen

$$1,\ 2,\ 3\ \ldots\ m$$

zu bestimmen, welche mit m den grössten gemeinschaftlichen Divisor δ haben.

Wir können dieselbe sogleich auf den früheren speciellen Fall zurückführen. Zunächst leuchtet nämlich ein, dass die Zahlen, um welche es sich handelt, unter den Vielfachen von δ, also unter den Zahlen

$$\delta,\ 2\delta,\ 3\delta,\ \ldots\ \frac{m}{\delta}\delta$$

zu suchen sind. Damit nun δ der grösste gemeinschaftliche Divisor von $m = \frac{m}{\delta}\delta$ und einer Zahl von der Form $r\delta$ sei, ist erforderlich und hinreichend, dass der Coefficient r relative Primzahl gegen $\frac{m}{\delta}$ sei; die gesuchte Anzahl ist daher zugleich die Anzahl derjenigen der Zahlen

$$1,\ 2,\ 3\ \ldots\ \frac{m}{\delta},$$

welche relative Primzahlen gegen die letzte $\frac{m}{\delta}$ derselben sind; diese Anzahl ist folglich $= \varphi\left(\frac{m}{\delta}\right)$. Offenbar geht diese allgemeinere Aufgabe wieder in die frühere über, wenn der Divisor $\delta = 1$ ist.

Aus der Lösung dieser Aufgabe lässt sich nun ein schöner Satz über die Function $\varphi(m)$ ableiten, der in späteren Untersuchungen eine grosse Rolle spielt. Schreiben wir einmal alle Divisoren

$$\delta',\ \delta'',\ \delta'''\ \ldots$$

der Zahl m auf, und theilen wir alle m Zahlen

$$1,\ 2,\ 3\ \ldots\ m$$

in ebenso viele Gruppen ein, als es Divisoren δ von m giebt, indem wir alle die Zahlen, welche mit m den grössten gemeinschaftlichen Divisor δ' haben und deren Anzahl nach dem Vorhergehenden $= \varphi\left(\frac{m}{\delta'}\right)$ ist, in die erste Gruppe, ebenso alle die $\varphi\left(\frac{m}{\delta''}\right)$ Zahlen, welche mit m den grössten gemeinschaftlichen Divisor δ'' haben, in die zweite Gruppe aufnehmen u. s. f. So leuchtet ein, dass jede der m Zahlen in eine, aber auch nur in eine solche Gruppe aufgenommen wird, und es muss daher das Aggregat der Zahlen

$$\varphi\left(\frac{m}{\delta'}\right), \quad \varphi\left(\frac{m}{\delta''}\right), \quad \varphi\left(\frac{m}{\delta'''}\right) \quad \ldots,$$

welche angeben, wie viele Zahlen der ersten, zweiten, dritten u. s. w. Gruppe angehören, mit der Anzahl m der sämmtlichen in diese Gruppen vertheilten Zahlen übereinstimmen. Wir erhalten daher den Satz

$$\varphi\left(\frac{m}{\delta'}\right) + \varphi\left(\frac{m}{\delta''}\right) + \varphi\left(\frac{m}{\delta'''}\right) + \cdots = m$$

oder

$$\Sigma\, \varphi\left(\frac{m}{\delta}\right) = m,$$

worin das Summenzeichen sich auf die sämmtlichen Divisoren δ der Zahl m bezieht. Es ist leicht, diesem Satze noch eine etwas andere Form zu geben; bedenkt man nämlich, dass, wenn für δ der Reihe nach alle Divisoren von m gesetzt werden, der Quotient $\frac{m}{\delta}$ ebenfalls jedesmal ein Divisor von m wird, und dass auf diese Weise $\frac{m}{\delta}$ jedem Divisor von m und jedem nur einmal gleich wird (denn verschiedenen Werthen von δ entsprechen auch verschiedene Werthe von $\frac{m}{\delta}$), so leuchtet ein, dass der Complex der Zahlen $\frac{m}{\delta}$ vollständig mit dem Complex der Divisoren δ übereinstimmt; wir können den obigen Satz daher auch so schreiben:

$$\Sigma\, \varphi(\delta) = m,$$

wo wieder das Summenzeichen sich auf alle Divisoren δ der Zahl m bezieht.

Es wird gut sein, diesen Satz wieder an einem Beispiel zu prüfen. Nehmen wir $m = 60$, so sind die Zahlen

$$1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 10,\ 12,\ 15,\ 20,\ 30,\ 60$$

die sämmtlichen Divisoren δ von 60. Nun ist

$$\begin{array}{llll} \varphi(1) = 1, & \varphi(2) = 1, & \varphi(3) = 2, & \varphi(4) = 2, \\ \varphi(5) = 4, & \varphi(6) = 2, & \varphi(10) = 4, & \varphi(12) = 4, \\ \varphi(15) = 8, & \varphi(20) = 8, & \varphi(30) = 8, & \varphi(60) = 16; \end{array}$$

und die Summe aller dieser Zahlen ist in der That $= 60$.

§. 14.

Der soeben gegebene Beweis dieses wichtigen Satzes über die Function $\varphi(m)$ ergab sich unmittelbar aus dem Begriff dieser Function ohne Hülfe der vorher für dieselbe gefundenen Form und ohne alle Rechnung*); es wird aber gut sein, noch einen zweiten Beweis hinzuzufügen, welcher mehr rechnend zu Werke geht und die früher abgeleitete Form der Function und die daraus gezogenen Folgerungen voraussetzt.

Jeder Divisor δ der Zahl

$$m = a^{\alpha}\, b^{\beta}\, c^{\gamma} \ \ldots$$

hat die Form

$$\delta = a^{\alpha'} b^{\beta'} c^{\gamma'} \ \ldots$$

wo wie früher $a, b, c \ldots$ von einander verschiedene Primzahlen bedeuten. Da also $a^{\alpha'}$, $b^{\beta'}$, $c^{\gamma'}$ ... unter einander relative Primzahlen sind, so ist

$$\varphi(\delta) = \varphi\left(a^{\alpha'}\right)\, \varphi\left(b^{\beta'}\right)\, \varphi\left(c^{\gamma'}\right) \ \ldots$$

Um nun alle Divisoren δ der Zahl m zu erhalten, muss man

*) Dieser Satz charakterisirt umgekehrt die Function $\varphi(m)$ vollständig, so dass aus ihm auch die (in §. 11 gefundene) Form derselben abgeleitet werden kann; siehe die Supplemente VII, §. 138.

α' die Zahlen $0, 1, 2 \ldots \alpha$
β' „ „ $0, 1, 2 \ldots \beta$
γ' „ „ $0, 1, 2 \ldots \gamma$
u. s. w.

durchlaufen lassen. Bildet man nun das Aggregat aller entsprechenden Werthe $\varphi(\delta)$, so leuchtet ein, dass dasselbe mit dem Product aus den folgenden Summen

$$\varphi(1) + \varphi(a) + \varphi(a^2) + \cdots + \varphi(a^\alpha)$$
$$\varphi(1) + \varphi(b) + \varphi(b^2) + \cdots + \varphi(b^\beta)$$
$$\varphi(1) + \varphi(c) + \varphi(c^2) + \cdots + \varphi(c^\gamma)$$
u. s. w.

übereinstimmt. Die erste dieser Summen ist aber gleich

$$1 + (a-1) + (a-1)\,a + \cdots + (a-1)\,a^{\alpha-1}$$
$$= 1 + (a^\alpha - 1) = a^\alpha;$$

ebenso ist b^β die zweite, c^γ die dritte Summe u. s. f. Es ergiebt sich daher, dass das Aggregat

$$\Sigma\,\varphi(\delta) = a^\alpha \cdot b^\beta \cdot c^\gamma \cdots = m$$

ist, was zu beweisen war.

§. 15.

Wir wenden uns nun noch zu einer Aufgabe, deren Lösung zu einem rein arithmetischen Beweise eines Satzes führt, welcher sonst gewöhnlich durch andere Betrachtungen erwiesen wird. Es handelt sich darum, wenn m eine beliebige ganze Zahl und p eine beliebige Primzahl ist, den Exponenten der höchsten Potenz von p zu bestimmen, welche in der Facultät

$$m! = 1 \cdot 2 \cdot 3 \cdots m$$

aufgeht. Bezeichnen wir mit m' die grösste in dem Bruch $\frac{m}{p}$ enthaltene ganze Zahl (so dass $m' \leqq \frac{m}{p} < m' + 1$), so sind unter den m Factoren von $m!$ nur die folgenden m' durch p theilbar

$$p,\ 2p,\ 3p \cdots m'p;$$

und da die übrigen Factoren bei unserer Frage keine Rolle spie-

len, so stimmt der gesuchte Exponent mit dem Exponenten der höchsten Potenz von p überein, welche in dem Product

$$1 \cdot 2 \quad . \quad . \quad . \quad m' \cdot p^{m'}$$

dieser Multipla von p aufgeht, und ist daher gleich der Summe aus m' und dem Exponenten der höchsten Potenz von p, welche in der Facultät

$$m'! = 1 \cdot 2 \quad . \quad . \quad . \quad m'$$

aufgeht. Hieraus ergiebt sich unmittelbar, dass der gesuchte Exponent gleich

$$m' + m'' + m''' + \quad . \quad . \quad .$$

ist, wo $m'', m''' \ldots$ die grössten in $\frac{m'}{p}, \frac{m''}{p} \ldots$ enthaltenen ganzen Zahlen bedeuten. Offenbar ist die Reihe der Zahlen $m', m'', m''' \ldots$ eine abnehmende, und folglich eine endliche; der gesuchte Exponent wird $= 0$ sein, wenn $p > m$ ist; denn dann ist schon $m' = 0$. Es mag beiläufig noch bemerkt werden, dass die Zahlen m', m'', $m''' \ldots$ auch die grössten resp. in $\frac{m}{p}, \frac{m}{p^2}, \frac{m}{p^3} \quad . \quad . \quad .$ enthaltenen ganzen Zahlen sind; ist nämlich r die grösste in $\frac{m}{a}$, und s die grösste in $\frac{r}{b}$ enthaltene ganze Zahl, so ist s auch stets die grösste in $\frac{m}{ab}$ enthaltene ganze Zahl.

Ist z. B. $m = 60$ und $p = 7$, so ist die grösste in

$$\frac{60}{7} \text{ enthaltene ganze Zahl } m' = 8$$

und die grösste in

$$\frac{8}{7} \text{ oder in } \frac{60}{49} \text{ enthaltene ganze Zahl } m'' = 1$$

und die grösste in

$$\frac{1}{7} \text{ oder in } \frac{60}{243} \text{ enthaltene ganze Zahl } m''' = 0;$$

also ist

$$7^{8+1} = 7^9$$

die höchste Potenz von 7, welche in der Facultät $60!$ aufgeht.

Durch das so gewonnene Resultat sind wir in den Stand gesetzt, folgenden Satz zu beweisen: Ist

$$m = f + g + h + \cdots,$$

so ist

$$\frac{m!}{f!\,g!\,h!\,\ldots}$$

eine ganze Zahl.

Denn wenn p irgend eine im Nenner aufgehende Primzahl ist, und wenn wir eine der frühern analoge Bezeichnung beibehalten, so sind

$$\begin{array}{l} f' + f'' + f''' + \cdots \\ g' + g'' + g''' + \cdots \\ h' + h'' + h''' + \cdots \\ \text{u. s. w.} \end{array}$$

die Exponenten der höchsten Potenzen von p, welche resp. in $f!$, in $g!$, in $h!$ u. s. w. aufgehen, und folglich ist

$$\begin{array}{c} (f' + g' + h' + \cdots) + (f'' + g'' + h'' + \cdots) \\ + (f''' + g''' + h''' + \cdots) + \cdots \end{array}$$

der Exponent der höchsten Potenz von p, welche in dem ganzen Nenner aufgeht. Andererseits ist

$$m' + m'' + m''' + \cdots$$

der Exponent der höchsten im Zähler aufgehenden Potenz von p; es ist daher nur zu zeigen, dass die letztere Summe nicht kleiner ist als die erstere. Da nun

$$\frac{m}{p} = \frac{f}{p} + \frac{g}{p} + \frac{h}{p} + \cdots$$

ist, so leuchtet unmittelbar ein, dass

$$m' \geqq f' + g' + h' + \cdots$$

sein muss; hieraus folgt aber wieder

$$\frac{m'}{p} \geqq \frac{f'}{p} + \frac{g'}{p} + \frac{h'}{p} + \cdots$$

also *a fortiori*

$$m'' \geqq f'' + g'' + h'' + \cdots$$

u. s. f., woraus die Richtigkeit der obigen Behauptung erhellt. Da nun jede im Nenner aufgehende Primzahl mindestens ebenso oft im Zähler aufgeht, so ist der Zähler theilbar durch den Nenner, der Bruch selbst also wirklich eine ganze Zahl*).

§. 16.

Hiermit beschliessen wir die Reihe der Sätze über die Theilbarkeit der Zahlen; aber es ist wohl der Mühe werth, an dieser Stelle noch einen Rückblick auf den Entwicklungsgang dieser unserer bisherigen Untersuchungen zu werfen. Da beobachten wir nun vor allen Dingen, dass das ganze Gebäude auf *einem* Fundament ruht, nämlich auf dem Algorithmus, welcher dazu dient, den grössten gemeinschaftlichen Theiler zweier Zahlen aufzufinden. Dass alle nachfolgenden Sätze, wenn sie sich auch zum Theil auf erst später eingeführte Begriffe, wie die der relativen und absoluten Primzahlen, beziehen, doch nur einfache Consequenzen aus dem Resultat jener ersten Untersuchung sind, ist so evident, dass man unmittelbar zu der Behauptung berechtigt wird: in jeder analogen Theorie, in welcher ein dem Algorithmus des grössten gemeinschaftlichen Divisors ähnlicher Algorithmus existirt, muss auch ein System von Folgerungen Statt finden, welches dem in unserer Theorie entwickelten ganz analog ist. In der That giebt es solche Theorieen; betrachtet man z. B. alle in der Form

$$t + u\sqrt{-a}$$

---

*) Hieraus folgt auch, dass jedes Product von m successiven ganzen Zahlen

$$(a+1)\,(a+2)\,\ldots\,(a+m-1)\,(a+m)$$

stets durch das Product der ersten m ganzen Zahlen

$$m! = 1\cdot 2\cdot 3\cdots(m-1)\,m$$

theilbar ist; denn der Quotient

$$\frac{(a+1)\,(a+2)\cdots(a+m-1)\,(a+m)}{1\;\cdot\;2\;\cdots\;(m-1)\;\;m}$$

ist gleich

$$\frac{(a+m)!}{a!\;m!}$$

und folglich eine ganze Zahl.

enthaltenen Zahlen, in welcher a eine bestimmte positive, t und u dagegen unbestimmte reelle ganze Zahlen bedeuten, und nennt dieselben ganze complexe Zahlen oder kurz ganze Zahlen, so kann man den Begriff des Vielfachen so fassen, dass eine solche Zahl ein Vielfaches von einer zweiten heisst, wenn die erste ein Product aus der zweiten und irgend einer dritten solchen Zahl ist. Aber nur für gewisse besondere Werthe von a, z. B. für $a = 1$, lässt sich die Frage nach den gemeinschaftlichen Divisoren zweier Zahlen durch einen endlich abschliessenden Algorithmus beantworten, der dem in unserer reellen Theorie ganz ähnlich ist; es findet daher in der Theorie der Zahlen von der Form $t + u\sqrt{-1}$ auch durchgängige Analogie mit unserer Theorie der reellen Zahlen Statt. Ganz anders verhält es sich, wenn z. B. $a = 11$ ist; in der Theorie der Zahlen von der Form $t + u\sqrt{-11}$ findet unter andern der Satz nicht mehr Statt, dass eine Zahl nur auf eine einzige Weise als Product von nicht weiter zerlegbaren Zahlen dargestellt werden kann; so z. B. lässt sich die Zahl 15 einmal als $3 \cdot 5$, ein anderes Mal als $(2 + \sqrt{-11})\,(2 - \sqrt{-11})$ darstellen, obgleich jede der vier Zahlen

$$3,\ 5,\ 2 + \sqrt{-11},\ 2 - \sqrt{-11}$$

nicht weiter in Factoren von der Form $t + u\sqrt{-11}$ zerlegbar ist. Der Grund dieser interessanten Erscheinung liegt allein darin, dass es bei den Zahlen dieser Form nicht mehr gelingt, einen nach einer endlichen Anzahl von Operationen abschliessenden Algorithmus zur Auffindung der gemeinschaftlichen Divisoren zweier Zahlen zu bilden *).

---

*) Die Einführung der ganzen complexen Zahlen von der Form $t + u\sqrt{-1}$ rührt von *Gauss* her; eine kurze Darstellung der Elemente dieser neuen Zahlentheorie findet man in seiner Abhandlung *Theoria residuorum biquadraticorum* II, oder in einer Abhandlung von *Dirichlet*: *Recherches sur les formes quadratiques à coëfficients et à indéterminées complexes* (Crelle's Journal XXIV). Das oben erwähnte abweichende Verhalten anderer Zahlformen hat *Kummer* zur Einführung der *idealen* Zahlen veranlasst (Crelle's Journal XXXV.).

Zweiter Abschnitt.

Von der Congruenz der Zahlen.

§. 17.

Bedeutet k irgend eine positive ganze Zahl, so lässt sich jede beliebige (positive oder negative) ganze Zahl a stets und nur auf eine einzige Weise in die Form

$$a = sk + r$$

bringen, in welcher s eine ganze Zahl und r eine der k Zahlen

$$0, \; 1, \; 2 \; . \; . \; . \; (k-1)$$

bedeutet. Denn lässt man zunächst s alle ganzen Zahlwerthe von $-\infty$ bis $+\infty$ durchlaufen, so bilden die Zahlen sk die sämmtlichen Multipla von k, und von einem solchen Multiplum sk bis zum nächst grössern $(s+1)k$ excl. giebt es immer nur k Zahlen, nämlich

$$sk, \; sk+1, \; sk+2 \; . \; . \; . \; sk+(k-1);$$

giebt man daher dem s alle denkbaren ganzen Zahlwerthe, und dem r jedesmal alle jene bestimmten k Werthe, so durchläuft der Ausdruck $sk + r$ wirklich alle ganzen Zahlwerthe a; dass ferner jede Zahl a auf diese Weise nur ein einziges Mal erzeugt wird, leuchtet auf folgende Weise ein. Wenn

$$s'k + r' = sk + r$$

ist, so folgt daraus

$$r' - r = (s - s')\,k;$$

wenn nun r' ebenfalls eine der k Zahlen $0, 1, 2 \ldots (k-1)$ ist, so ist der absolute Werth von $r' - r$ ebenfalls eine dieser Zahlen, also kleiner als k; da aber $r' - r$ ein Multiplum von k ist, so kann $r' - r$ nur $= 0$ sein, woraus $r' = r$ und $s' = s$ folgt.

Wir werden nun im Folgenden sagen, dass die Zahl r der *Rest* der Zahl a in Bezug auf den *Modulus* k ist; sobald ferner zwei Zahlen a und b in Bezug auf denselben Modulus k denselben Rest r lassen, sollen sie *gleichrestig* oder (nach *Gauss*) *congruent* in Bezug auf den Modulus k heissen; da in diesem Fall $a = sk + r$ und $b = s'k + r$ ist, so folgt, dass die Differenz $a - b = (s - s')k$ durch den Modulus k theilbar ist; und umgekehrt, ist $a - b$ durch k theilbar, so sind die Zahlen a und b auch congruent in Bezug auf den Modul k; denn ist r der Rest von a, r' der von b, also

$$a = sk + r, \quad b = s'k + r',$$

so ist

$$a - b = (s - s')\,k + (r - r');$$

da nun der Voraussetzung nach $a - b$ ein Multiplum von k ist, so muss auch $r' - r$ ein solches sein, was, wie wir vorher gesehen haben, nicht anders möglich ist, als wenn $r' = r$ ist. Man könnte daher congruente Zahlen auch als solche definiren, deren Differenz durch den Modul theilbar ist. (Aus diesem Grunde hat man die Bedeutung des Wortes Rest in der Weise erweitert, dass jede von zwei einander nach dem Modul k congruenten Zahlen a und b ein *Rest* der andern heisst.)

Da man sehr häufig die Congruenz zweier Zahlen a und b in Bezug auf eine dritte k als Modul auszudrücken hat, so ist von *Gauss* für dieselbe ein eigenes Zeichen eingeführt; man schreibt nämlich

$$a \equiv b \pmod{k}.$$

So ist z. B.

$$3 \equiv -25 \pmod{4}, \quad 65 \equiv 16 \pmod{7}.$$

Da die beiden Zahlen a und b in dem Begriffe der Congruenz dieselbe Rolle spielen, so darf man offenbar die zur Linken und Rechten des Zeichens $\equiv$ stehenden Zahlen mit einander vertauschen.

Ferner leuchten aus dem Begriffe der Congruenz leicht die folgenden Sätze ein:

1) Sind a und k zwei beliebige Zahlen, so ist stets

$$a \equiv a \pmod{k}.$$

2) Ist in Bezug auf denselben Modulus k eine erste Zahl a einer zweiten b, diese wieder einer dritten c congruent, so ist auch die erste a der dritten c in Bezug auf k congruent; in Zeichen: ist

$$a \equiv b \pmod{k}, \quad b \equiv c \pmod{k},$$

so ist auch

$$a \equiv c \pmod{k}.$$

Denn die Reste der drei Zahlen a, b, c sind einander gleich; oder auch, da $a - b$ und $b - c$ Multipla von k sind, so ist auch $(a - b) + (b - c) = a - c$ Multiplum von k.

3) Ist

$$a \equiv b \pmod{k} \text{ und } m \equiv n \pmod{k},$$

so ist auch

$$a + m \equiv b + n \pmod{k} \text{ und } a - m \equiv b - n \pmod{k}.$$

Denn da $a - b$ und $m - n$ Multipla von k sind, so sind auch $(a - b) + (m - n) = (a + m) - (b + n)$ und $(a - b) - (m - n) = (a - m) - (b - n)$ Multipla von k.

Dies lässt sich für eine beliebige Anzahl von Congruenzen erweitern, die sich auf denselben Modulus beziehen; man kann sie addiren und subtrahiren wie Gleichungen.

4) Ist wieder

$$a \equiv b \pmod{k} \text{ und } m \equiv n \pmod{k},$$

so ist auch

$$am \equiv bn \pmod{k}.$$

Denn da $a - b$ ein Vielfaches von k ist, so ist zunächst auch $(a - b)m = am - bm$ ein solches, also

$$am \equiv bm \pmod{k};$$

da ferner $m-n$ ein Vielfaches von k ist, so ist auch $b\,(m-n) = bm - bn$ ein solches, also

$$bm \equiv bn \pmod{k};$$

die beiden Zahlen am und bn sind daher derselben Zahl bm congruent, folglich sind sie auch unter einander congruent.

Auch dieser Satz lässt sich dahin verallgemeinern, dass man eine ganze Reihe von Congruenzen, die sich auf denselben Modul beziehen, mit einander multipliciren kann wie Gleichungen; und hieraus folgt wieder, dass gleich hohe Potenzen zweier congruenten Zahlen wieder congruent sind in Bezug auf denselben Modulus.

5) Die bisherigen Sätze kann man folgendermaassen zusammenfassen. Ist $f(x, y, z \ldots)$ eine ganze rationale Function der Unbestimmten $x, y, z \ldots$, deren Coefficienten ganze Zahlen sind, und ist in Bezug auf einen und denselben Modulus k

$$a \equiv a', \quad b \equiv b', \quad c \equiv c' \quad \ldots,$$

so ist auch

$$f(a, b, c \ldots) \equiv f(a', b', c' \ldots) \pmod{k}.$$

6) Etwas anders verhält es sich bei der Division. Ist nämlich

$$am \equiv bm \pmod{k},$$

so kann man hieraus im Allgemeinen nicht mit Sicherheit schliessen, dass auch $a \equiv b \pmod{k}$ sein muss; bezeichnen wir mit δ den grössten gemeinschaftlichen Divisor der beiden Zahlen m und k, so folgt aus der obigen Congruenz nur, dass

$$a \equiv b \left(\text{mod.}\ \frac{k}{\delta}\right)$$

sein muss. Denn da $m\,(a-b)$ durch k, also $\frac{m}{\delta}(a-b)$ durch $\frac{k}{\delta}$ theilbar, und $\frac{m}{\delta}$ relative Primzahl gegen $\frac{k}{\delta}$ ist, so muss $(a-b)$ durch $\frac{k}{\delta}$ theilbar sein.

7) Ist

$$a \equiv b \pmod{k}$$

und m irgend ein Divisor von k, so ist auch

$$a \equiv b \pmod{m}.$$

Denn $a - b$ ist ein Multiplum von k, und k ein Multiplum von m; also ist $a - b$ auch ein Multiplum von m.

8) Ist

$$a \equiv b \pmod{k} \text{ und } a \equiv b \pmod{l} \text{ und } a \equiv b \pmod{m}, \text{ u. s. w.}$$

so ist auch

$$a \equiv b \pmod{h},$$

wo h das kleinste gemeinschaftliche Multiplum von $k, l, m \ldots$ bezeichnet. Denn $a - b$ ist ein gemeinschaftliches Multiplum aller dieser Zahlen, also auch Multiplum von h.

Hieraus folgt auch noch als ein besonders bemerkenswerther specieller Fall, dass, wenn eine Congruenz richtig ist in Bezug auf eine Reihe von Moduln, die sämmtlich unter einander relative Primzahlen sind, dieselbe auch in Bezug auf einen Modul gilt, welcher das Product aus allen jenen Moduln ist.

§. 18.

Da jede beliebige Zahl a ihrem Reste r in Bezug auf den Modul k congruent ist, so ist jede Zahl a einer der k Zahlen

$$0, \; 1, \; 2 \; . \; . \; . \; (k-1)$$

congruent; sie kann aber auch nur einer dieser Zahlen congruent sein, denn sonst müssten ja auch unter diesen k Resten mindestens zwei einander congruent sein, was offenbar nicht der Fall ist. Theilen wir daher sämmtliche Zahlen in *Classen* ein nach dem Princip, dass wir jedesmal zwei Zahlen in dieselbe oder in verschiedene Classen werfen, je nachdem sie in Bezug auf den Modulus k congruent sind oder nicht, so ist die *Anzahl* dieser Classen offenbar $= k$; die eine enthält sämmtliche Zahlen, welche $\equiv 0 \pmod{k}$, d. h. durch k theilbar sind; die folgende Classe enthält alle Zahlen, welche $\equiv 1 \pmod{k}$ sind, u. s. f.

Greift man nun aus jeder dieser Classen nach Belieben ein Individuum heraus, so hat das so gebildete System von k Zahlen die charakteristische Eigenschaft, dass jede beliebige ganze Zahl

stets einer und auch nur einer von diesen k Zahlen congruent ist; ein solches System, wie es z. B. auch die Zahlen

$$0, 1, 2 \ldots (k-1)$$

bilden, nennt man ein *vollständiges System nicht congruenter* (oder *incongruenter*) *Zahlen* oder ein *vollständiges Restsystem* in Bezug auf den Modul k; offenbar bilden auch die Zahlen

$$1, 2, 3 \ldots k$$

und ebenso je k successive ganze Zahlen ein solches System.

Alle Zahlen, welche einer und derselben Classe angehören, haben nun mehrere allen gemeinschaftliche Eigenschaften, so dass sie in Bezug auf den Modul fast die Rolle einer einzigen Zahl spielen. Wir haben schon früher gesehen, dass jede Zahl, welche in einer Congruenz als Summand oder als Factor auftritt, unbeschadet der Richtigkeit der Congruenz durch jede andere ihr congruente, d. h. derselben Classe angehörige Zahl ersetzt werden darf. Ein anderes Element, welches allen in einer Classe enthaltenen Individuen gemeinschaftlich ist, bildet der grösste Divisor, den sie mit dem Modul k gemeinschaftlich haben; denn sind a und b zwei congruente Zahlen, so ist

$$a = b + sk,$$

und folglich ist jeder gemeinschaftliche Divisor von a und k auch gemeinschaftlicher Divisor von b und k. Man kann daher nach diesem grössten gemeinschaftlichen Divisor die Classen wieder in Gruppen eintheilen, und da die Zahlen

$$1, 2 \ldots k$$

ein vollständiges System incongruenter Zahlen bilden, so ist, wenn δ irgend einen Divisor von k bezeichnet, $\varphi\left(\frac{k}{\delta}\right)$ die Anzahl derjenigen Classen, welche solche Zahlen enthalten, die δ zum grössten gemeinschaftlichen Divisor mit dem Modul k haben. Speciell ist also $\varphi(k)$ die Anzahl derjenigen Classen, welche nur Zahlen enthalten, die relative Primzahlen gegen den Modulus k sind.

Von besonderer Wichtigkeit für spätere Untersuchungen ist auch noch folgender Satz:

Ist a relative Primzahl gegen den Modulus k, und setzt man in dem linearen Ausdruck $ax + b$ *für x der Reihe nach alle k Glieder*

eines vollständigen Systems incongruenter Zahlen ein, so bilden die so entstehenden Werthe dieses Ausdrucks wieder ein vollständiges System incongruenter Zahlen.

Da nämlich aus

$$ax + b \equiv ay + b \pmod{k}$$

auch

$$ax \equiv ay \pmod{k}$$

und, da a relative Primzahl gegen k ist, nach §. 17, 6) auch

$$x \equiv y \pmod{k}$$

folgt, so ergiebt sich, dass alle Werthe des Ausdrucks $ax + b$, welche incongruenten Werthen von x entsprechen, ebenfalls incongruent sind; setzt man daher für x alle k incongruenten Zahlen ein, so erhält der Ausdruck $ax + b$ auch k incongruente Werthe, welche, da es überhaupt nur k Classen giebt, ein vollständiges System incongruenter Zahlen bilden.

§. 19.

Betrachten wir jetzt den Ausdruck ax, in welchem a wieder relative Primzahl gegen den Modul k ist, und setzen wir wieder für x der Reihe nach die Glieder eines vollständigen Systems incongruenter Zahlen ein, aber nicht alle, sondern nur diejenigen

$$a_1,\ a_2,\ a_3\ \ldots,$$

welche relative Primzahlen gegen den Modul k sind, und deren Anzahl nach dem vorigen Paragraphen gleich $\varphi(k)$ ist, so leuchtet erstens ein, dass die Werthe des Ausdrucks ax, d. h. die Producte

$$aa_1,\ aa_2,\ aa_3\ \ldots$$

sämmtlich incongruent sind, ferner, dass dieselben sämmtlich wieder relative Primzahlen gegen k sind; es wird daher jedes dieser Producte einem und nur einem Gliede der Reihe

$$a_1,\ a_2,\ a_3\ \ldots$$

congruent sein. Wir können daher setzen

$$\left.\begin{aligned} aa_1 &\equiv b_1 \\ aa_2 &\equiv b_2 \\ aa_3 &\equiv b_3 \\ \text{u. s. w.} & \end{aligned}\right\} \pmod{k},$$

wo nun die Zahlen

$$b_1, \; b_2, \; b_3 \; \ldots$$

vollständig, wenn auch in anderer Ordnung, mit den Zahlen

$$a_1, \; a_2, \; a_3 \; \ldots$$

übereinstimmen, so dass namentlich

$$a_1 a_2 a_3 \ldots = b_1 b_2 b_3 \ldots$$

sein wird. Bezeichnen wir zur Abkürzung dieses Product mit P, und multipliciren wir die vorstehenden $\varphi(k)$ Congruenzen mit einander, so erhalten wir daher

$$a^{\varphi(k)} \cdot P \equiv P \pmod{k}.$$

Nun ist aber P ein Product von lauter Zahlen, die relative Primzahlen gegen den Modul sind, also selbst relative Primzahl gegen den Modul k; es ist daher nach §. 17, 6) gestattet, die vorstehende Congruenz durch den gemeinschaftlichen Factor P beider Seiten ohne Weiteres zu dividiren. Auf diese Weise erhalten wir die Congruenz

$$a^{\varphi(k)} \equiv 1 \pmod{k};$$

in Worten kann man diesen höchst wichtigen Satz folgendermaassen aussprechen:

Ist a relative Primzahl gegen die positive Zahl k, und erhebt man a zu einer Potenz, deren Exponent $\varphi(k)$ angiebt, wie viele der Zahlen

$$1, \; 2, \; 3 \; \ldots \; k$$

relative Primzahlen gegen k sind, so lässt diese Potenz, durch k dividirt, stets den Rest 1.

Nehmen wir z. B. $k = 15$, $a = 2$, so ist a wirklich relative Primzahl gegen k; nun ist $\varphi(k) = \varphi(15) = \varphi(3)\,\varphi(5) = 8$; es muss daher 2^8, durch 15 dividirt, den Rest 1 lassen; in der That ist

$$2^8 = 256 = 17 \cdot 15 + 1.$$

Es kann übrigens vorkommen, dass auch Potenzen von a mit niedrigerm Exponenten als $\varphi(k)$ denselben Rest 1 geben. Dies tritt wirklich in dem eben gewählten Beispiel ein, denn es ist auch

$$2^4 = 16 = 1 \cdot 15 + 1.$$

Specialisiren wir unsern Satz für den Fall, dass k nur durch eine einzige Primzahl p theilbar, also

$$k = p^\pi, \quad \varphi(k) = (p-1)\, p^{\pi-1}$$

ist, so erhalten wir den Satz:

Ist p eine Primzahl und a irgend eine durch p nicht theilbare Zahl, so ist

$$a^{(p-1)p^{\pi-1}} \equiv 1 \pmod{p^\pi}.$$

Nehmen wir ferner hierin $\pi = 1$, so erhalten wir einen berühmten Satz, der zuerst von *Fermat* aufgestellt ist und daher der Fermat'sche Satz heisst:

Ist p eine Primzahl und a irgend eine durch p nicht theilbare Zahl, so ist

$$a^{p-1} \equiv 1 \pmod{p}.$$

Man kann diesen Satz so umformen, dass er auch für den Fall gültig bleibt, wenn a durch p theilbar ist; zu diesem Zweck braucht man nur die vorstehende Congruenz mit a zu multipliciren, wodurch sie in die folgende

$$a^p \equiv a \pmod{p}$$

übergeht. Ist nämlich a theilbar durch p, so sind beide Seiten dieser Congruenz $\equiv 0 \pmod{p}$, also ist sie auch dann noch richtig. Umgekehrt kann man aus dieser Form des Satzes auch wieder die frühere ableiten; denn sobald a nicht theilbar durch p, also relative Primzahl gegen p ist, darf man beide Seiten dieser Congruenz auch wieder durch a dividiren, ohne den Modul zu ändern.

Kehren wir zu dem allgemeinen Satz zurück, der zuerst von *Euler* bewiesen ist und den Namen des verallgemeinerten Fermat'schen Satzes führt, so können wir denselben auch in folgender Weise aussprechen: Sind $p, r, s \ldots$ von einander verschiedene absolute Primzahlen, und ist a durch keine dieser Primzahlen theilbar, so ist stets

$$a^{(p-1)p^{\pi-1} \cdot (r-1)r^{\varrho-1} \cdot (s-1)s^{\sigma-1} \cdots} \equiv 1 \pmod{p^\pi r^\varrho s^\sigma \ldots},$$

worin $\pi, \varrho, \sigma \ldots$ irgend welche ganze positive Zahlen bedeuten.

§. 20.

Es ist wohl nicht überflüssig, dem vorhergehenden Beweise dieses wichtigen Satzes einen zweiten hinzuzufügen, der gradatim zu Werke geht und sich zunächst auf den binomischen Satz stützt. Ist p irgend eine ganze positive Zahl, so ist zufolge dieses Satzes bekanntlich

$$(a+b)^p =$$
$$a^p + \frac{p}{1} a^{p-1} b + \cdots + \frac{p!}{r!(p-r)!} a^{p-r} b^r + \cdots + b^p;$$

hierin sind (nach §. 15) alle Coefficienten ganze Zahlen. Ist aber p eine Primzahl, so können wir hinzufügen, dass alle Coefficienten mit Ausnahme des ersten und letzten, welche $= 1$ sind, durch p theilbar sind; denn der Zähler des Bruches

$$\frac{p!}{r!(p-r)!},$$

in welchem r eine der Zahlen $1, 2, 3 \ldots (p-1)$ bedeutet, enthält den Factor p, der Nenner dagegen nicht; er ist also von der Form $\frac{pm}{n}$, wo n nicht theilbar durch p, also auch relative Primzahl gegen p ist; da wir aber ferner wissen, dass dieser Bruch eine ganze Zahl, dass also pm durch n theilbar ist, so muss m durch n theilbar sein; der Bruch hat daher die Form $p \cdot \frac{m}{n}$, wo der zweite Factor eine ganze Zahl ist; und folglich ist jeder dieser $(p-1)$ Coefficienten $\equiv 0 \pmod{p}$. Sind daher a und b irgend welche ganze Zahlen, so erhalten wir die folgende Congruenz

$$(a+b)^p \equiv a^p + b^p \pmod{p},$$

wobei also vorausgesetzt ist, dass p eine Primzahl ist. Offenbar folgt hieraus weiter

$$(a+b+c)^p \equiv (a+b)^p + c^p \equiv a^p + b^p + c^p \pmod{p}$$

und allgemein für eine beliebige Reihe von n ganzen Zahlen a, $b \ldots h$:

$$(a+b+\cdots+h)^p \equiv a^p + b^p + \cdots + h^p \pmod{p}.$$

Setzen wir hierin $a = 1$, $b = 1 \ldots h = 1$, so erhalten wir für jede beliebige positive ganze Zahl n den Satz:

$$n^p \equiv n \pmod{p}.$$

Da ferner für jede ungerade Primzahl $(-1)^p \equiv -1$, und für die einzige gerade Primzahl $p = 2$ ebenfalls $(-1)^p = 1 \equiv -1 \pmod{p}$ ist, so erhalten wir durch Multiplication der vorstehenden Congruenz mit der andern

$$(-1)^p \equiv -1 \pmod{p}$$

die neue

$$(-n)^p \equiv -n \pmod{p}.$$

Also ist der Fermat'sche Satz

$$a^p \equiv a \pmod{p}$$

für jede positive und negative Zahl a bewiesen, während er für $a = 0$ unmittelbar evident ist. Wenn nun a nicht durch p theilbar ist, was wir von jetzt annehmen wollen, so folgt hieraus, dass

$$a^{p-1} \equiv 1 \pmod{p}, \text{ d. h. } a^{p-1} = 1 + hp$$

ist, wo h eine ganze Zahl bedeutet. Erheben wir diese Gleichung zur $p$ten Potenz und entwickeln die rechte Seite wieder nach dem binomischen Satze, so zeigt sich, dass alle Glieder mit Ausnahme des ersten Multipla von p^2 sind; wir erhalten daher

$$a^{(p-1)p} = 1 + h'p^2 \text{ oder } a^{(p-1)p} \equiv 1 \pmod{p^2},$$

wo wieder h' eine ganze Zahl bedeutet. So kann man fortfahren, indem man jedesmal wieder zur $p$ten Potenz erhebt, und gelangt auf diese Weise zu der Congruenz

$$a^{(p-1)p^{\pi-1}} \equiv 1 \pmod{p^\pi},$$

deren Allgemeingültigkeit sich in derselben Weise durch den Schluss von π auf $\pi + 1$ nachweisen lässt.

Sind nun $r, s \ldots$ ebenfalls Primzahlen, welche nicht in a aufgehen, so ist nach demselben Satze

$$a^{(r-1)r^{\varrho-1}} \equiv 1 \pmod{r^\varrho}, \quad a^{(s-1)s^{\sigma-1}} \equiv 1 \pmod{s^\sigma} \quad \ldots$$

Setzen wir ferner zur Abkürzung

$$h = (p-1)p^{\pi-1} \cdot (r-1)r^{\varrho-1} \cdot (s-1)s^{\sigma-1} \ldots$$

und berücksichtigen wir, dass aus jeder Congruenz von der Form

$$a^{\alpha} \equiv 1 \pmod{m}$$

auch die Congruenz

$$a^{h} \equiv 1 \pmod{m}$$

folgt, sobald h ein Multiplum von α ist, so ergiebt sich, dass die Congruenz

$$a^{h} \equiv 1$$

für jeden der Moduln $p^{\pi}, r^{\varrho}, s^{\sigma} \ldots$ und folglich, da dieselben relative Primzahlen sind, auch für den Modul

$$k = p^{\pi}\, r^{\varrho}\, s^{\sigma} \quad \ldots$$

gilt. Hiermit ist also von Neuem der verallgemeinerte Fermat'sche Satz erwiesen.

§. 21.

Es kommt häufig vor, dass eine oder beide Seiten einer Congruenz eine oder mehrere unbestimmte Zahlen $x, y \ldots$ enthalten, und es wird dann die Aufgabe gestellt, alle ganzzahligen Werthe von $x, y \ldots$ zu suchen, durch welche die beiden Seiten der Congruenz wirklich einander congruent werden. Je nach der Anzahl der Unbestimmten $x, y \ldots$ heisst dann eine solche Congruenz eine Congruenz mit einer, zwei oder mehreren *Unbekannten*, ähnlich wie dies bei Gleichungen zu geschehen pflegt. Auch hier nennt man dann solche specielle Werthe von $x, y \ldots$, welche die Congruenz zu einer identischen machen, *Wurzeln* der Congruenz, und das Problem der Auflösung einer Congruenz besteht in der Auffindung ihrer sämmtlichen Wurzeln. Wir werden im Folgenden nur solche Congruenzen betrachten, welche eine einzige Unbekannte x enthalten und ausserdem sich auf die Form

$$ax^{m} + bx^{m-1} + \cdot \cdot \cdot + gx + h \equiv 0 \pmod{k}$$

bringen lassen, worin m eine positive ganze Zahl und $a, b \ldots g, h$ ebenfalls gegebene ganze Zahlen bedeuten. Jeder Werth von x, der, in die linke Seite eingesetzt, dieselbe durch den Modul k theilbar macht, heisst also eine Wurzel dieser Congruenz. Kennt

man irgend eine solche Wurzel x, so sind offenbar nach §. 17, 5) alle ihr nach dem Modul k congruenten Zahlen, d. h. alle Individuen der Classe, welcher diese Zahl x angehört, ebenfalls Wurzeln derselben Congruenz; man sieht alle solche einander congruenten Wurzeln daher nur wie eine einzige Wurzel an, und das Problem der vollständigen Auflösung der Congruenz kommt daher darauf zurück, alle unter einander *incongruenten* Wurzeln derselben aufzufinden.

Ferner leuchtet ein, dass jede Wurzel der obigen Congruenz, sobald

$$a \equiv a',\ b \equiv b' \ \ldots\ g \equiv g',\ h \equiv h' \pmod{k}$$

ist, auch eine Wurzel der Congruenz

$$a'x^m + b'x^{m-1} + \cdots + g'x + h' \equiv 0 \pmod{k}$$

sein wird, und umgekehrt. Beide Congruenzen sind daher auch nur wie eine und dieselbe anzusehen; denn beide stellen an die Unbekannte x genau dieselbe Forderung. Hieraus erhellt unmittelbar, dass man aus jeder Congruenz von der obigen Form ohne Weiteres alle diejenigen Glieder fortstreichen darf, deren Coefficienten durch den Modul theilbar sind; der Exponent der höchsten Potenz von x. welche nach dieser vorläufigen Ausscheidung zurückbleibt, heisst dann der *Grad* dieser Congruenz; ist z. B. in der obigen Congruenz der erste Coefficient a nicht durch den Modul k theilbar, so heisst dieselbe eine Congruenz $m$ten Grades.

Wenden wir diese Benennungen z. B. auf die Congruenz

$$x^{\varphi(k)} \equiv 1 \pmod{k}$$

an, so müssen wir sagen, dass dieselbe genau ebenso viele (incongruente) Wurzeln besitzt, als ihr Grad $\varphi(k)$ Einheiten enthält; denn erstens genügen alle relativen Primzahlen gegen den Modul der Congruenz, und diese zerfallen in $\varphi(k)$ Classen; und zweitens kann die Congruenz keine andern Wurzeln haben als diese; denn der grösste gemeinschaftliche Divisor δ einer Wurzel x und des Modul k ist auch gemeinschaftlicher Divisor der Zahlen $x^{\varphi(k)}$ und k, folglich auch (§. 18) der Zahlen 1 und k; folglich kann δ nur $= 1$ sein.

§. 22.

Wir wenden uns nun nach den vorhergehenden allgemeinen Erörterungen zu dem einfachsten speciellen Fall, nämlich zu der Congruenz ersten Grades, welcher man offenbar durch Transposition des bekannten Gliedes stets die Form

$$ax \equiv b \pmod{k} \tag{1}$$

geben kann. Betrachten wir auch hier zunächst nur den speciellen Fall, in welchem der Coefficient a relative Primzahl gegen den Modul k ist, so ergiebt sich unmittelbar, dass diese Congruenz stets eine, aber auch nur eine Wurzel hat. Denn wir haben früher (§. 18) gesehen, dass die Werthe des Ausdrucks ax, welche man erhält, wenn man für x sämmtliche k Individuen eines vollständigen Systems incongruenter Zahlen einsetzt, wieder ein solches System bilden; unter den Werthen dieses Ausdrucks wird sich daher auch einer und nur einer finden, welcher derselben Classe angehört wie b, d. h. welcher $\equiv b$ ist. Der verallgemeinerte Fermat'sche Satz giebt nun auch ein Mittel an die Hand, die Wurzel dieser Congruenz unmittelbar zu bestimmen; offenbar genügt jede Zahl

$$x \equiv b \,.\, a^{\varphi(k)-1} \pmod{k}$$

der obigen Congruenz. So findet man z. B., dass alle Wurzeln der Congruenz

$$2x \equiv -3 \pmod{15}$$

durch die Formel

$$x \equiv -3 \,.\, 2^7 \equiv 6 \pmod{15}$$

gegeben werden.

Wenden wir uns nun dem allgemeinen Fall zu und nehmen wir an, es sei δ der grösste gemeinschaftliche Divisor des Coefficienten a und des Modul k, so leuchtet zunächst ein, dass, wenn die Congruenz überhaupt eine Wurzel x besitzt, auch b durch δ theilbar sein muss; denn da ax mit dem Modul k den gemeinschaftlichen Divisor δ hat, so muss auch $b \equiv ax$ durch δ theilbar sein. Dies ist also eine unerlässliche Bedingung für die Möglichkeit der Congruenz; dass sie auch hinreichend für dieselbe ist, wird sich sogleich zeigen.

Gesetzt nun, es sei x eine Wurzel der Congruenz, also

$$ax = b + mk,$$

wo m irgend eine ganze Zahl, so folgt hieraus

$$\frac{a}{\delta} x = \frac{b}{\delta} + m \frac{k}{\delta},$$

d. h. jede Wurzel der ursprünglichen Congruenz ist auch Wurzel der Congruenz

$$\frac{a}{\delta} x \equiv \frac{b}{\delta} \left(\text{mod.} \frac{k}{\delta}\right) \tag{2}$$

und umgekehrt überzeugt man sich sogleich, dass jede Wurzel dieser letztern Congruenz auch eine Wurzel der erstern sein wird; denn aus

$$\frac{a}{\delta} x = \frac{b}{\delta} + m \frac{k}{\delta}$$

folgt auch wieder

$$ax = b + mk.$$

Die beiden Congruenzen (1) und (2) stimmen daher hinsichtlich ihrer Wurzeln vollständig mit einander überein; da nun in der letztern der Coefficient $\frac{a}{\delta}$ relative Primzahl gegen den Modul $\frac{k}{\delta}$ ist, so haben wir wieder den frühern Fall: diese Congruenz ist stets lösbar, und alle ihr genügenden Zahlen bilden in Bezug auf ihren Modul $\frac{k}{\delta}$ nur eine einzige Classe, in der Weise, dass, wenn α eine bestimmte derselben ist, alle andern in der Form

$$x = \alpha + z \frac{k}{\delta} \tag{3}$$

enthalten sind, wo z jede beliebige ganze Zahl bedeutet. Da nun alle diese Zahlen auch die sämmtlichen Wurzeln der Congruenz (1) bilden, so fragt es sich nur noch, wie viele in Bezug auf den Modul k incongruente Zahlen unter ihnen sich vorfinden. Irgend zwei in der Reihe (3) enthaltene Zahlen

$$\alpha + z \frac{k}{\delta} \text{ und } \alpha + z' \frac{k}{\delta}$$

werden offenbar stets und auch nur dann congruent in Bezug auf den Modulus k sein, sobald

$$(z' - z)\frac{k}{\delta}$$

durch k, und also $z' - z$ durch δ theilbar ist; diese beiden Zahlen werden also einer und derselben Classe, oder verschiedenen Classen in Bezug auf den Modul k angehören, je nachdem die beiden Zahlen z und z' einer und derselben Classe, oder verschiedenen Classen in Bezug auf den Modulus δ angehören; woraus unmittelbar folgt, dass die Reihe (3) sämmtliche Individuen von δ verschiedenen Classen in Bezug auf den Modul k enthält, und es leuchtet ein, dass die folgenden δ Zahlen

$$\alpha,\ \alpha + \frac{k}{\delta},\ \alpha + 2\frac{k}{\delta} \dots \alpha + (\delta - 1)\frac{k}{\delta}$$

aus jeder dieser δ Classen einen Repräsentanten enthalten. Wir haben mithin folgendes allgemeine Resultat gewonnen:

Damit die Congruenz

$$ax \equiv b \pmod{k}$$

überhaupt Wurzeln besitze, ist erforderlich, dass b durch den grössten gemeinschaftlichen Divisor δ der beiden Zahlen a und k theilbar sei; ist diese Bedingung erfüllt, so hat die Congruenz genau δ incongruente Wurzeln.

Es ist zu bemerken, dass in dem früher behandelten Fall, in welchem $\delta = 1$ ist, die erforderliche Bedingung stets erfüllt ist, ferner, dass dieser Satz auch noch für den Fall $\delta = k$, in welchem also $a \equiv 0 \pmod{k}$ ist, seine Gültigkeit behält, indem, sobald b ebenfalls $\equiv 0 \pmod{k}$ ist, jede beliebige Zahl x dieser identischen Congruenz Genüge leistet.

Um auch ein Beispiel für den allgemeinen Fall zu behandeln, nehmen wir die Congruenz

$$8x \equiv -12 \pmod{60};$$

der grösste gemeinschaftliche Divisor des Coefficienten 8 und des Modul 60 ist hier $= 4$; da die rechte Seite -12 durch denselben theilbar ist, so ist sie möglich und wird 4 nach dem Modul 60 incongruente Wurzeln haben. Wir finden dieselben, indem wir zunächst die Wurzeln der entsprechenden Congruenz

$$2x \equiv -3 \pmod{15}$$

suchen; wir haben oben gesehen, dass dieselben in der Form

$$x \equiv 6 \pmod{15}$$

enthalten sind, und schliessen daraus, dass

$$x \equiv 6, \quad \equiv 21, \quad \equiv 36, \quad \equiv 51 \pmod{60}$$

die vier Wurzeln der ursprünglichen Congruenz sind.

§. 23.

Obgleich im Vorhergehenden das Problem, zu entscheiden, ob eine vorgelegte Congruenz ersten Grades Wurzeln hat oder nicht, und im erstern Fall dieselben aufzufinden, eine vollständige Lösung gefunden hat, so ist dieselbe, sobald der Modul k eine grosse Zahl ist, wegen der erforderlichen Potenzirung für praktische Zwecke nicht wohl anwendbar; wir wollen daher im Folgenden eine einfachere Methode angeben. Offenbar können wir uns auf den Fall beschränken, in welchem der Coefficient der Unbekannten relative Primzahl gegen den Modul ist; ausserdem können wir annehmen, dass die rechte Seite $= 1$ ist; denn um aus der Wurzel einer solchen Congruenz diejenige einer andern zu finden, in welcher die rechte Seite eine andere Zahl ist, genügt es offenbar, dieselbe mit dieser Zahl zu multipliciren. Nennen wir der Bequemlichkeit halber den Modul nicht k, sondern b, so reducirt sich also unsere Aufgabe auf die Auflösung der Congruenz

$$ax \equiv 1 \pmod{b}$$

oder, was dasselbe ist, auf die Auflösung der unbestimmten Gleichung ersten Grades

$$ax - by = 1.$$

Wir schicken derselben einige Sätze über einen Algorithmus voraus, der zuerst von *Euler* behandelt und für die Theorie der Kettenbrüche, sowie auch für unsere spätern Untersuchungen von Wichtigkeit ist. Es seien

$$a, \quad b \qquad (1)$$

irgend zwei unbestimmte Grössen, und ebenso

$$\gamma,\ \delta,\ \varepsilon\ \ldots\ \lambda,\ \mu,\ \nu \tag{2}$$

eine Reihe von beliebig vielen unbestimmten Grössen. Aus diesen bilden wir nun successive eine neue Reihe $c, d, e \ldots l, m, n$ nach folgendem Gesetz:

$$c = \gamma b + a,\ d = \delta c + b,\ e = \varepsilon d + c \ldots n = \nu m + l. \tag{3}$$

Substituirt man den Ausdruck für c in den für d, so wird der letztere eine ähnliche Form annehmen wie der erstere, nämlich

$$d = \delta a + (\gamma\delta + 1)\, b;$$

er besteht also aus einem Gliede, welches den Factor a, und aus einem zweiten, welches den Factor b enthält. Substituirt man nun diesen Ausdruck für d, und den ersten für c in den Ausdruck für e, so nimmt auch dieser letztere dieselbe Form an. So kann man fortfahren, und aus dem Ausdruck für n erkennt man, dass dieses Gesetz allgemein ist; denn sobald l und m schon diese Form erhalten haben, so nimmt auch n dieselbe an. Wir können daher

$$n = Ga + Hb$$

setzen, wo nun G und H unabhängig von a und b sein werden. Man bezeichnet den Coefficienten H, der nur von den in der Reihe (2) befindlichen Grössen abhängt, durch das Zeichen

$$[\gamma,\ \delta,\ \varepsilon\ \ldots\ \lambda,\ \mu,\ \nu] \tag{4}$$

und wir werden im Folgenden einige interessante Sätze beweisen, die sich auf dasselbe beziehen.

Zunächst leuchtet ein, dass, wenn man mit den Anfangsgliedern

$$b,\ c = \gamma b + a \tag{1'}$$

und der Reihe

$$\delta,\ \varepsilon\ \ldots\ \lambda,\ \mu,\ \nu \tag{2'}$$

in derselben Weise verfährt wie oben, man genau dieselben Glieder $d, e \ldots l, m, n$ erhalten wird. Wir können daher gleichzeitig

$$n = Ga + [\gamma,\ \delta,\ \varepsilon\ \ldots\ \mu,\ \nu]\ b$$

und

$$n = G'b + [\delta,\ \varepsilon\ \ldots\ \mu,\ \nu]\ c$$

setzen; ersetzen wir hierin c durch $\gamma b + a$, so erhalten wir

$$n = [\delta, \varepsilon \ldots \mu, \nu]\, a + (\gamma\, [\delta, \varepsilon \ldots \mu, \nu] + G')\, b,$$

woraus durch Vergleichung der Coefficienten von a in beiden Formen von n zunächst

$$G = [\delta, \varepsilon \ldots \mu, \nu]$$

folgt. Der Coefficient G lässt sich daher durch dasselbe Zeichen ausdrücken wie H. Wir können also von jetzt an schreiben

$$n = [\delta \ldots \mu, \nu]\, a + [\gamma, \delta \ldots \mu, \nu]\, b;$$

da nun auch

$$G' = [\varepsilon \ldots \mu, \nu]$$

sein muss, so erhalten wir durch Vergleichung der Coefficienten von b in den beiden Formen für n den Satz

$$[\gamma, \delta, \varepsilon \ldots \nu] = \gamma\, [\delta, \varepsilon \ldots \nu] + [\varepsilon \ldots \nu], \tag{5}$$

in welchem das Gesetz ausgedrückt ist, nach welchem die Fortbildung der Ausdrücke von der Form (4) nach links hin geschieht.

Einen ganz analogen Satz für die Fortbildung nach rechts hin erhält man durch die einfache Bemerkung, dass durch die Annahme $a = 0$, $b = 1$ die drei Grössen l, m, n resp. in

$$[\gamma \ldots \lambda],\ [\gamma \ldots \lambda, \mu],\ [\gamma \ldots \lambda, \mu, \nu]$$

übergehen, so dass zwischen diesen drei consecutiven Ausdrücken die Relation

$$[\gamma \ldots \lambda, \mu, \nu] = [\gamma \ldots \lambda, \mu]\, \nu + [\gamma \ldots \lambda] \tag{6}$$

besteht.

Verbindet man diese beiden Sätze mit einander, so überzeugt man sich leicht von der Richtigkeit des folgenden:

$$[\nu, \mu \ldots \delta, \gamma] = [\gamma, \delta \ldots \mu, \nu]. \tag{7}$$

Nimmt man nämlich an, dieser Satz sei für alle Ausdrücke dieser Art bewiesen, welche eine kleinere Anzahl von Grössen enthalten, so dass also z. B.

$$[\delta, \varepsilon \ldots \nu] = [\nu \ldots \varepsilon, \delta] \text{ und } [\varepsilon \ldots \nu] = [\nu \ldots \varepsilon]$$

so folgt aus (5):

$$[\gamma, \delta, \varepsilon \ldots \nu] = [\nu \ldots \varepsilon, \delta]\, \gamma + [\nu \ldots \varepsilon];$$

verbindet man dies mit dem Satz (6), so ergiebt sich unmittelbar die Richtigkeit der Gleichung (7). In der That gilt aber der Satz wirklich für die ersten Fälle; enthält nämlich der Ausdruck nur eine einzige Grösse γ, so versteht sich dies von selbst; und ausserdem ist

$$[\gamma, \delta] = \gamma\delta + 1 = [\delta, \gamma].$$

Hieraus folgt also, dass der Satz auch für jede beliebige Anzahl der Grössen $\gamma, \delta \ldots \mu, \nu$ gilt.

Wir können die Gleichungen (3), durch welche das Bildungsgesetz der Grössen $c, d \ldots n$ ausgedrückt wird, auch in folgender Weise schreiben:

$$-c = (-\gamma)\, b + (-a),\ + d = (-\delta)\,(-c) + b,$$
$$-e = (-\varepsilon)\, d + (-c) \ldots \pm n = (-\nu)\,(\mp m) + (\pm l),$$

wo in der letzten Gleichung das obere oder untere Zeichen zu nehmen ist, je nachdem die Anzahl der Grössen $\gamma, \delta \ldots \mu, \nu$ gerade oder ungerade ist. Hieraus geht hervor, dass aus den Anfangsgliedern

$$-a,\ b \tag{1''}$$

und der Reihe

$$-\gamma,\ -\delta,\ -\varepsilon \ldots -\lambda,\ -\mu,\ -\nu \tag{2''}$$

durch dasselbe frühere Verfahren die Reihe

$$-c,\ +d,\ -e \ldots \pm n$$

entsteht. Es wird daher auch

$$\pm n = [-\delta, -\varepsilon \ldots -\nu]\,(-a) + [-\gamma, -\delta, -\varepsilon \ldots -\nu]\, b$$

und folglich

$$[-\gamma, -\delta \ldots -\nu] = \pm [\gamma, \delta \ldots \nu] \tag{8}$$

sein, worin wieder das obere oder untere Zeichen zu nehmen ist, je nachdem die Anzahl der Grössen $\gamma, \delta \ldots \nu$ gerade oder ungerade ist.

Endlich kann man die Gleichungen (3) auch in umgekehrter Folge so schreiben:

$$l = (-\nu)\, m + n, \quad k = (-\mu)\, l + m \ldots$$
$$b = (-\delta)\, c + d, \quad a = (-\gamma)\, b + c.$$

Es wird daher

$$a = [-\mu \ldots -\gamma]\, n + [-\nu, -\mu \ldots -\gamma]\, m$$

oder mit Hülfe des Satzes (8):

$$\pm a = -[\mu \ldots \gamma]\, n + [\nu, \mu \ldots \gamma]\, m$$

oder mit Berücksichtigung des Satzes (7):

$$\pm a = -[\gamma, \delta \ldots \mu]\, n + [\gamma, \delta \ldots \mu, \nu]\, m.$$

Wenn man nun $a = 1$, $b = 0$ setzt, so gehen m, n resp. in

$$[\delta \ldots \mu], \quad [\delta \ldots \mu, \nu]$$

über, und man erhält das Resultat:

$$[\delta \ldots \mu]\ [\gamma, \delta \ldots \mu, \nu] - [\delta \ldots \mu, \nu]\ [\gamma, \delta \ldots \mu] = \pm 1, \qquad (9)$$

wo wieder das obere oder untere Zeichen zu nehmen ist, je nachdem die Anzahl der Grössen $\gamma, \delta \ldots \mu, \nu$ gerade oder ungerade ist.

Zum Schluss wollen wir bemerken, dass diese Ausdrücke in der Theorie der Kettenbrüche von der grössten Wichtigkeit sind; es ist nämlich

$$\gamma + \cfrac{1}{\delta + \cfrac{1}{\varepsilon + \ddots + \cfrac{1}{\mu + \cfrac{1}{\nu}}}} = \frac{[\gamma, \delta, \varepsilon \ldots \mu, \nu]}{[\delta, \varepsilon \ldots \mu, \nu]} \qquad (10)$$

Denn gesetzt, dieser Satz sei schon für jede kleinere Anzahl der Grössen $\gamma, \delta, \varepsilon \ldots \mu, \nu$ bewiesen, so dass also namentlich

$$\delta + \cfrac{1}{\varepsilon + \ddots \cfrac{1}{\nu}} = \frac{[\delta, \varepsilon \ldots \mu, \nu]}{[\varepsilon \ldots \mu, \nu]}$$

ist, so folgt hieraus als Werth der linken Seite der Gleichung (10)

$$\gamma + \frac{[\varepsilon \ldots \mu, \nu]}{[\delta, \varepsilon \ldots \mu, \nu]} = \frac{\gamma\, [\delta, \varepsilon \ldots \mu, \nu] + [\varepsilon \ldots \mu, \nu]}{[\delta, \varepsilon \ldots \mu, \nu]}$$

und hieraus ergiebt sich mit Berücksichtigung des Satzes (5) die Richtigkeit des Satzes (10). In der That ist aber

$$\gamma + \frac{1}{\delta} = \frac{\gamma\delta + 1}{\delta} = \frac{[\gamma, \delta]}{[\delta]};$$

da also der Satz für zwei Grössen γ, δ richtig ist, so ist er auch für jede beliebige Anzahl der Grössen $\gamma, \delta \ldots \mu, \nu$ richtig.

Sind die Elemente $\gamma, \delta \ldots \mu, \nu$ ganze Zahlen, so gilt dasselbe von den Zählern und Nennern der Brüche

$$\frac{[\gamma]}{1}, \frac{[\gamma, \delta]}{[\delta]} \ldots \frac{[\gamma, \delta \ldots \mu, \nu]}{[\delta \ldots \mu, \nu]};$$

ferner ist jeder dieser Brüche irreductibel, d. h. durch die kleinsten Zahlen ausgedrückt; denn es folgt z. B. aus der Relation (9), dass Zähler und Nenner des letzten der obigen Brüche ohne gemeinschaftlichen Divisor sind.

§. 24.

Die vorstehenden Sätze sind deshalb gleich in solcher Vollständigkeit aufgestellt, damit wir bei einer spätern Untersuchung nicht nöthig haben, von Neuem auf denselben Algorithmus zurückzukommen; für unsern nächsten Bedarf, nämlich für die Lösung der unbestimmten Gleichung

$$ax - by = 1,$$

in welcher wir nun wieder a und b als zwei gegebene relative Primzahlen ansehen, genügt schon ein kleiner Theil der vorhergehenden Resultate. Zu dem Zweck verfahren wir nun, wie es bei der Aufsuchung des grössten gemeinschaftlichen Divisors der beiden Zahlen (oder bei der Verwandlung des Bruches $\frac{a}{b}$ in einen Kettenbruch) geschieht, indem wir das System der folgenden Gleichungen bilden:

$$a = \gamma b + c, \quad b = \delta c + d \ldots$$

und so fort, bis wir endlich in der Gleichung

$$l = \nu m + 1$$

zu dem Rest 1 gelangen, was ja geschehen muss; diese Gleichungen können wir auch so schreiben

$$c = (-\gamma)\, b + a;\ d = (-\delta)\, c + b \ldots 1 = (-\nu)\, m + l$$

und hieraus folgt, dass

$$1 = [-\delta, -\varepsilon \ldots -\mu, -\nu]\, a + [-\gamma, -\delta, -\varepsilon \ldots -\mu, -\nu]\, b$$

oder

$$1 = \mp [\delta, \varepsilon \ldots \mu, \nu]\, a \pm [\gamma, \delta, \varepsilon \ldots \mu, \nu]\, b$$

ist, worin das obere oder untere Zeichen zu nehmen ist, je nachdem die Anzahl der Grössen $\gamma, \delta \ldots \mu, \nu$ gerade oder ungerade ist. Wir erhalten daher folgende Auflösung der unbestimmten Gleichung:

$$x = \mp [\delta, \varepsilon \ldots \mu, \nu],\ \ y = \mp [\gamma, \delta, \varepsilon \ldots \mu, \nu].$$

Hiermit ist also auch eine Wurzel x der Congruenz

$$ax \equiv 1 \pmod{b}$$

gefunden, und dies genügt vollständig, da alle andern dieser einen nach dem Modul b congruent sind*).

Wenden wir diese Methode auf unser Beispiel

$$2x \equiv 1 \pmod{15}$$

an, so erhalten wir

$$2 = 0\,.\,15 + 2,\ \ 15 = 7\,.\,2 + 1$$

also

$$\gamma = 0,\ \ \delta = 7,\ \ x \equiv -[\delta] \equiv -7 \equiv 8 \pmod{15}$$

und hieraus folgt, dass

$$x \equiv -7\,.\,(-3) \equiv 21 \equiv 6 \pmod{15}$$

die Wurzel der Congruenz

$$2x \equiv -3 \pmod{15}$$

ist.

---

*) Man überzeugt sich leicht, dass aus einer Lösung x_0, y_0 alle andern sich durch die Gleichungen $x = x_0 + bz$, $y = y_0 + az$ ableiten lassen, wo z eine willkürliche ganze Zahl bedeutet.

Als zweites Beispiel wählen wir die Congruenz

$$37x \equiv 1 \pmod{100};$$

indem wir ebenso verfahren, erhalten wir

$$37 = 0 \cdot 100 + 37;\ 100 = 2 \cdot 37 + 26;\ 37 = 1 \cdot 26 + 11;$$
$$26 = 2 \cdot 11 + 4;\ 11 = 2 \cdot 4 + 3;\ 4 = 1 \cdot 3 + 1$$

und also

$$x \equiv -[2, 1, 2, 2, 1] \pmod{100}.$$

Nun ist, wenn wir von rechts nach links rechnen,

$$[1] = 1,\ [2, 1] = 3\ \ [2, 2, 1] = 7,\ [1, 2, 2, 1] = 10,$$
$$[2, 1, 2, 2, 1] = 27,$$

also

$$x \equiv -27 \equiv 73 \pmod{100}.$$

Da $\varphi(100) = \varphi(4)\,\varphi(25) = 2 \cdot 20 = 40$ ist, so hätten wir nach unserer früheren Methode die Auflösung

$$x \equiv 37^{39} \pmod{100}$$

erhalten; die hierin angedeutete Rechnung würde sich zwar durch einige Kunstgriffe bedeutend abkürzen lassen, allein doch viel langwieriger sein als die nach der zweiten Methode ausgeführte Rechnung.

Kommt es darauf an, auch den Werth von

$$y = \mp [\gamma, \delta, \varepsilon \ldots \mu, \nu]$$

zu berechnen, so ist es vortheilhaft, die Berechnung des Werthes

$$x = \mp [\delta, \varepsilon \ldots \mu, \nu]$$

von rechts nach links vorzunehmen; man findet dann nach der Formel (5) des §. 23 aus

$$[\varepsilon \ldots \mu, \nu] \text{ und } [\delta, \varepsilon \ldots \mu, \nu]$$

unmittelbar den Werth von y. So oft $\gamma = 0$, also $a < b$ ist, reducirt sich y auf

$$y = \mp [\varepsilon \ldots \mu, \nu].$$

Dies ist in unsern Beispielen der Fall; in dem zweiten erhält man auf diese Weise

$$y = -[0, 2, 1, 2, 2, 1] = -[1, 2, 2, 1] = -10,$$

und in der That ist

$$37 \cdot (-27) - 100 \cdot (-10) = 1 .$$

§. 25.

Auf das im Vorhergehenden behandelte Problem der Auflösung der Congruenzen ersten Grades lässt sich das folgende zurückführen:

Alle Zahlen x zu finden, welche in Bezug auf zwei gegebene Moduln a, b gegebenen Zahlen resp. α, β congruent sind, d. h. welche den beiden Forderungen

$$x \equiv \alpha \pmod{a}, \quad x \equiv \beta \pmod{b}$$

genügen.

Da nämlich alle Zahlen x, welche die erste dieser beiden Forderungen erfüllen, in der Form $x = \alpha + at$ enthalten sind, wo t jede beliebige ganze Zahl bedeutet, so kommt es nur noch darauf an, dieses t näher so zu bestimmen, dass

$$at \equiv \beta - \alpha \pmod{b} \tag{1}$$

wird. Bezeichnet man nun mit δ den grössten gemeinschaftlichen Divisor der beiden Moduln a und b, so muss, wenn diese Congruenz möglich sein soll, $\beta - \alpha$ durch δ theilbar, d. h. es muss

$$\alpha \equiv \beta \pmod{\delta} \tag{2}$$

sein. Ist diese Bedingung nicht erfüllt, so existirt keine Zahl, welche der Aufgabe genügt; ist sie aber erfüllt, so sind sämmtliche der Congruenz (1) genügende Zahlen t in der Form

$$t \equiv \gamma \left(\text{mod.}\, \frac{b}{\delta}\right) \text{ oder } t = \gamma + \frac{b}{\delta}\, u$$

enthalten, wo γ eine bestimmte von ihnen, und u jede beliebige ganze Zahl bedeutet. Hieraus folgt, dass die gesuchten Zahlen durch die Formel

$$x = \alpha + \gamma a + \frac{ab}{\delta}\, u \text{ oder } x \equiv x_0 \left(\text{mod.}\, \frac{ab}{\delta}\right)$$

gegeben werden, wo $x_0 = \alpha + \gamma a$ selbst eine der gesuchten

Zahlen, und $\frac{ab}{\delta}$ offenbar das kleinste gemeinschaftliche Multiplum der beiden gegebenen Moduln a, b ist.

Werden z. B. die Zahlen gesucht, welche durch 12 dividirt den Rest 7, durch 15 dividirt den Rest 4 lassen, so hat man die Congruenzen

$$x \equiv 7 \pmod{12}, \quad x \equiv 4 \pmod{15}.$$

Man setzt also $x = 7 + 12t$, und erhält für t die Congruenz

$$12t \equiv -3 \pmod{15},$$

welche (da hier die Bedingung (2) erfüllt ist) sich auf

$$4t \equiv -1 \pmod{5}$$

reducirt. Hieraus folgt

$$t \equiv 1 \pmod{5}$$

und also

$$x = 7 + 12t \equiv 19 \pmod{60}.$$

Besonders bemerkenswerth ist der besondere Fall, in welchem die beiden gegebenen Moduln a, b relative Primzahlen sind; da gleichzeitig $\delta = 1$ wird, so fällt die Bedingung (2) ganz fort; die Auflösung ist stets möglich und liefert ein Resultat von der Form

$$x \equiv x_0 \pmod{ab}.$$

Die ursprüngliche Aufgabe lässt sich auch leicht für den Fall verallgemeinern, in welchem eine Reihe von beliebig vielen Moduln und eine Reihe ihnen entsprechender Reste gegeben ist; für uns ist indessen nur der Fall von Wichtigkeit, in welchem je zwei der gegebenen Moduln $a, b, c \dots$ relative Primzahlen unter einander sind; wir beschränken uns daher auf denselben, und stellen uns unter dieser Voraussetzung die Aufgabe, alle Zahlen x zu finden, welche dem System von Congruenzen

$$x \equiv \alpha \pmod{a}, \quad x \equiv \beta \pmod{b}, \quad x \equiv \gamma \pmod{c} \dots$$

genügen. Da wir nun schon wissen, dass alle Zahlen, welche die beiden ersten dieser Forderungen erfüllen, in der Form $x \equiv \beta_1 \pmod{ab}$ enthalten sind, wo die Zahl β_1 nach dem Vorhergehen-

den gefunden werden kann, so kommt unsere Aufgabe offenbar auf die einfachere zurück, alle Zahlen x zu finden, welche dem folgenden System von Congruenzen genügen:

$$x \equiv \beta_1 \text{ (mod. } ab), \quad x \equiv \gamma \text{ (mod. } c) \ldots$$

Da nun der Modul ab der ersten dieser Congruenzen wieder relative Primzahl gegen jeden folgenden Modul $c \ldots$ ist, so kann man in derselben Weise fortfahren und gelangt so zu dem Resultat, dass sämmtliche Zahlen x in der Form

$$x \equiv x_0 \text{ (mod. } m)$$

enthalten sind, wo x_0 eine bestimmte von ihnen, und m das Product $abc \ldots$ aus allen gegebenen Moduln bedeutet.

Statt eine solche Zahl x_0 in der eben angegebenen Weise durch successive Auflösung einer Reihe von Congruenzen ersten Grades in Bezug auf die Moduln $b, c \ldots$ zu suchen, kann man auch auf folgende Art symmetrisch verfahren. Man suche zunächst Zahlen $r, s, t \ldots$, welche den folgenden Paaren von Congruenzen genügen:

$$r \equiv 1 \text{ (mod. } a); \quad s \equiv 1 \text{ (mod. } b); \quad t \equiv 1 \text{ (mod. } c) \cdots$$

$$r \equiv 0 \left(\text{mod.} \frac{m}{a}\right); \quad s \equiv 0 \left(\text{mod.} \frac{m}{b}\right); \quad t \equiv 0 \left(\text{mod.} \frac{m}{c}\right) \cdots$$

wo m wieder zur Abkürzung für das Product $abc \ldots$ gesetzt ist; da a relative Primzahl gegen $\frac{m}{a} = bc \ldots$ ist, und Aehnliches von den folgenden Congruenzen-Paaren gilt, so sind dieselben stets möglich und nach der obigen Methode lösbar; und sobald diese Zahlen $r, s, t \ldots$ gefunden sind, wird die gesuchte Auflösung durch die Congruenz

$$x \equiv \alpha r + \beta s + \gamma t + \cdots \text{ (mod. } m)$$

gegeben; denn da z. B. in Bezug auf den Modul a

$$r \equiv 1, \quad s \equiv 0, \quad t \equiv 0 \ldots$$

ist, so ergiebt sich wirklich $x \equiv \alpha$ (mod. a); ebenso $x \equiv \beta$ (mod. b) u. s. f. Ein besonderer Vortheil dieser Methode besteht darin, dass die Hülfszahlen $r, s, t \ldots$ ganz unabhängig von $\alpha, \beta, \gamma \ldots$ sind, und daher stets dieselben bleiben, wie auch die letztern variiren

mögen, vorausgesetzt natürlich, dass das System der Moduln $a, b, c \ldots$ unverändert bleibt.

Es folgt ferner hieraus, dass x ein vollständiges Restsystem nach dem Modul m durchläuft, sobald die Reste $\alpha, \beta, \gamma \ldots$ vollständige Restsysteme resp. in Bezug auf die Moduln $a, b, c \ldots$ durchlaufen; denn, wenn $\alpha', \beta', \gamma' \ldots$ irgend ein zweites System gegebener Reste ist, so wird

$$\alpha' r + \beta' s + \gamma' t + \cdots$$

stets und nur dann

$$\equiv \alpha r + \beta s + \gamma t + \cdots$$

nach dem Modulus m sein, wenn gleichzeitig

$$\alpha' \equiv \alpha \text{ (mod. } a), \quad \beta' \equiv \beta \text{ (mod. } b), \quad \gamma' \equiv \gamma \text{ (mod. } c)$$

u. s. w. ist; da ferner $\alpha, \beta, \gamma \ldots$ resp. $a, b, c \ldots$ verschiedene Werthe durchlaufen, so ist die Anzahl aller verschiedenen Restsysteme, also auch die Anzahl der resultirenden nach dem Modul m incongruenten Werthe von x gleich $abc \ldots = m$; d. h. x durchläuft ein vollständiges Restsystem nach dem Modul m.

Ist ferner α relative Primzahl zu a, β zu b u. s. f., so ist x auch relative Primzahl zu m, und umgekehrt; hieraus folgt leicht ein neuer Beweis des Satzes, dass $\varphi(ab) = \varphi(a)\,\varphi(b)$ ist.

Endlich ergiebt sich, dass, wenn x irgend eine ganze Zahl bedeutet, stets

$$\frac{x}{m} = h + \frac{a'}{a} + \frac{b'}{b} + \frac{c'}{c} + \cdots$$

gesetzt werden kann, wo $h, a', b', c' \ldots$ ganze Zahlen bedeuten.

§. 26.

Wir wenden uns nun zu der Betrachtung der Congruenzen höherer Grade, beschränken uns aber dabei auf den einfachsten Fall, in welchem der Modul p eine *Primzahl* ist. Die allgemeinste Form einer Congruenz $n$ten Grades ist die folgende:

$$ax^n + bx^{n-1} + cx^{n-2} + \cdots + h \equiv 0 \text{ (mod. } p),$$

in welcher der höchste Coefficient a als nicht theilbar durch die

Primzahl p vorausgesetzt wird. Ebenso wie man jede Gleichung leicht auf den Fall zurückführen kann, in welchem der höchste Coefficient $= 1$ ist, so erreicht man auch hier dasselbe, wenn man die Congruenz mit einer Zahl a' multiplicirt, welche der Bedingung $aa' \equiv 1 \pmod{p}$ genügt und also eine Wurzel der stets lösbaren Congruenz $ax \equiv 1 \pmod{p}$ ist. Doch hängt hiervon die Gültigkeit der folgenden Sätze nicht im Mindesten ab.

Wir bezeichnen der Einfachheit halber das auf der linken Seite der obigen Congruenz befindliche Polynom $n$ten Grades kurz mit $f(x)$. Hat nun eine solche Congruenz

$$f(x) \equiv 0 \pmod{p} \tag{1}$$

eine Wurzel $x \equiv \alpha$, und dividirt man $f(x)$ durch $x - \alpha$, so wird der Divisionsrest r_1 eine durch p theilbare Zahl sein; denn bezeichnet man den Quotienten der Division, welcher eine ganze Function vom $(n-1)$ten Grade mit ganzzahligen Coefficienten ist, mit $f_1(x)$, so ist

$$f(x) = (x - \alpha)\, f_1(x) + r_1 \tag{2}$$

und hierin ist $r_1 = f(\alpha)$ der Voraussetzung nach $\equiv 0 \pmod{p}$.

Hat nun die Congruenz (1) noch eine zweite von α verschiedene, d. h. nicht mit α congruente Wurzel β, so folgt aus (2), dass

$$(\beta - \alpha)\, f_1(\beta) \equiv 0 \pmod{p}$$

und also, da $\beta - \alpha$ nicht durch p theilbar ist, dass $f_1(\beta) \equiv 0$, d. h. dass β eine Wurzel der Congruenz $f_1(x) \equiv 0 \pmod{p}$ sein muss. Man kann daher wieder

$$f_1(x) = (x - \beta)\, f_2(x) + r_2$$

setzen, wo der Rest r_2 wieder eine durch p theilbare Zahl, und der Quotient $f_2(x)$ eine ganze Function $(n-2)$ten Grades mit ganzzahligen Coefficienten ist. Setzt man aber diesen Ausdruck für $f_1(x)$ in die Gleichung (2) ein, so nimmt dieselbe die Form

$$f(x) = (x - \alpha)(x - \beta)\, f_2(x) + r_2(x - \alpha) + r_1$$

oder, da r_1 und r_2 durch p theilbar sind, die Form

$$f(x) = (x - \alpha)(x - \beta)\, f_2(x) + p(lx + m)$$

an, in welcher l und m ganze Zahlen sind.

Besitzt nun die Congruenz (1) noch eine dritte von α und β verschiedene Wurzel γ, so ergiebt sich, da weder $(\gamma - \alpha)$ noch $(\gamma - \beta)$ durch p theilbar ist, dass γ eine Wurzel der Congruenz $f_2(x) \equiv 0$ ist; verfährt man daher wie früher, so erhält man eine Gleichung von der Form

$$f(x) = (x - \alpha)(x - \beta)(x - \gamma) f_3(x) + p(rx^2 + sx + t),$$

wo r, s, t ganze Zahlen bedeuten.

Gesetzt nun, die Congruenz (1) besitze mindestens eben so viele unter einander incongruente Wurzeln $\alpha, \beta, \gamma \ldots \lambda$, als ihr Grad n Einheiten enthält, so sieht man, dass die Fortsetzung desselben Verfahrens endlich zu einer Gleichung von der Form

$$f(x) = a(x - \alpha)(x - \beta)(x - \gamma) \cdots (x - \lambda) + p\psi(x) \quad (3)$$

führt, wo a der höchste Coefficient der Polynome $f(x)$, $f_1(x)$, $f_2(x) \ldots$ ist, und $\psi(x)$ ein Polynom bedeutet, dessen Coefficienten sämmtlich ganze Zahlen sind.

Aus diesem ersten Satze folgt sogleich der zweite, dass eine Congruenz (deren Modul immer als Primzahl vorausgesetzt wird) nie mehr incongruente Wurzeln haben kann, als ihr Grad Einheiten enthält. Denn hätte die Congruenz (1) ausser den n Wurzeln $\alpha, \beta \ldots \lambda$ noch mindestens eine solche μ, die mit keiner der vorhergehenden congruent ist, so würde aus der Gleichung (3) folgen, dass das Product

$$a(\mu - \alpha)(\mu - \beta)(\mu - \gamma) \ldots (\mu - \lambda)$$

durch p theilbar wäre, was unmöglich ist, da der Voraussetzung nach keiner der Factoren durch p theilbar ist.

Man hätte diese beiden Sätze, welche für die Folge von der grössten Wichtigkeit sind, auch in umgekehrter Folge aus dem in der Gleichung (2) ausgesprochenen Resultat schliessen können. Da nämlich jede von α verschiedene Wurzel β der Congruenz (1) eine Wurzel der Congruenz nächst niedrigern Grades

$$f_1(x) \equiv 0 \pmod{p}$$

ist, so folgt hieraus unmittelbar, dass die erstere Congruenz höchstens eine Wurzel mehr besitzt, als die letztere; da nun eine Congruenz ersten Grades (sobald der Modulus eine Primzahl ist) nur eine Wurzel besitzt, so kann eine Congruenz vom 2ten Grade

höchstens 2, folglich eine Congruenz dritten Grades höchstens 3 u. s. f. allgemein eine Congruenz $n$ten Grades höchstens n incongruente Wurzeln besitzen. Und nachdem so der zweite Satz bewiesen ist, ergiebt sich auch der erste leicht auf folgende Weise. Gesetzt, die Congruenz (1) vom $n$ten Grade hat wirklich n incongruente Wurzeln $\alpha, \beta, \gamma \ldots \lambda$, so bilde man die Differenz

$$f(x) - a\,(x-\alpha)\,(x-\beta)\,(x-\gamma)\cdots(x-\lambda) = \varphi(x)$$

wo a den höchsten Coefficienten in $f(x)$ bezeichnet, und denke sich dieselbe nach Potenzen von x geordnet; dann ist zu zeigen, dass alle Coefficienten dieses Polynoms $\varphi(x)$, dessen Grad höchstens $= n-1$, also jedenfalls kleiner als n ist, durch p theilbar sind. Gesetzt, dies wäre nicht der Fall, und es wäre x^r die höchste in $\varphi(x)$ vorkommende Potenz von x, deren Coefficient nicht durch p theilbar wäre, so wäre

$$\varphi(x) \equiv 0 \pmod{p}$$

eine Congruenz vom $r$ten Grade, welche, wie man unmittelbar einsieht, die n incongruenten Zahlen $\alpha, \beta \ldots \lambda$ zu Wurzeln hätte, also, da $r < n$ ist, mehr Wurzeln besässe, als ihr Grad Einheiten enthält. Da dies gegen den schon bewiesenen Satz streitet, so müssen wirklich alle Coefficienten von $\varphi(x)$ durch p theilbar sein, d. h. es muss

$$\varphi(x) = p\,\psi(x)$$

sein, wo sämmtliche Coefficienten des Polynoms $\psi(x)$ ganze Zahlen sind. Dies war aber der Inhalt des ersten Satzes.

Wir können zu diesen beiden Sätzen noch den folgenden dritten hinzufügen: Wenn

$$f(x) = \varphi(x)\,\psi(x)$$

ist, wo die Coefficienten der Polynome $\varphi(x)$ und $\psi(x)$ sämmtlich ganze Zahlen sind, und wenn die Congruenz

$$f(x) \equiv 0 \pmod{p}, \tag{4}$$

(wo p wieder eine Primzahl bedeutet) ebenso viele incongruente Wurzeln besitzt als ihr Grad Einheiten enthält, so gilt dasselbe von jeder der beiden Congruenzen

$$\varphi(x) \equiv 0 \pmod{p}, \quad \psi(x) \equiv 0 \pmod{p}. \tag{5}$$

Zunächst leuchtet nämlich ein, dass jede Wurzel α der Congruenz (4) auch eine Wurzel von mindestens einer der beiden Congruenzen (5) sein muss; denn aus

$$\varphi(\alpha)\ \psi(\alpha) = f(\alpha) \equiv 0 \pmod{p}$$

folgt, dass mindestens eine der beiden Zahlen $\varphi(\alpha)$, $\psi(\alpha)$ durch p theilbar sein muss. Hätte nun eine der beiden Congruenzen (5) weniger incongruente Wurzeln als ihr Grad Einheiten enthält, so müsste nothwendig die Anzahl der Wurzeln der andern Congruenz d. h. der übrigen Wurzeln der Congruenz (4) ihren Grad übersteigen, da die Summe der Grade der beiden Polynome $\varphi(x)$ und $\psi(x)$ genau dem Grade des Polynoms $f(x)$ gleich ist. Da dies gegen den zweiten Satz verstossen würde, so muss die Anzahl der incongruenten Wurzeln einer jeden der beiden Congruenzen (5) genau ihrem Grade gleich sein.

§. 27.

Von diesen wichtigen Sätzen machen wir sogleich eine Anwendung. Zufolge des Fermat'schen Satzes genügt jede der $(p-1)$ unter einander nach dem Modul p incongruenten Zahlen

$$1,\ 2,\ 3\ \ldots\ (p-1)$$

der Congruenz

$$x^{p-1} - 1 \equiv 0 \pmod{p},$$

und diese Zahlen bilden auch ihre sämmtlichen incongruenten Wurzeln. Es ist daher nach dem ersten der vorhergehenden drei Sätze

$$x^{p-1} - 1 = (x-1)\ (x-2)\ (x-3)\ \ldots\ (x-p+1) + p\,\psi(x),$$

worin $\psi(x)$ ein Polynom mit ganzen Coefficienten bezeichnet. Entwickelt man daher das rechter Hand befindliche Product nach Potenzen von x, so muss der Coefficient einer jeden Potenz von x dem entsprechenden linker Hand in Bezug auf den Modul p congruent sein. Wir wollen hier nur den interessantesten Fall betrachten, der sich durch die Vergleichung der Glieder ergiebt, welche von x unabhängig sind. Ist zunächst p eine *ungerade* Primzahl, so ist dieses Glied rechter Hand, da die Anzahl $p-1$ der negativen Factoren gerade ist,

$$= 1 \cdot 2 \cdot 3 \cdots (p-1),$$

linker Hand dagegen $= -1$, und hieraus ergiebt sich der nach *Wilson* benannte Satz:

Wenn p eine Primzahl bedeutet, so ist das um eine Einheit vergrösserte Product aller kleinern Zahlen als p durch p theilbar; in Zeichen

$$1 \cdot 2 \cdots (p-1) \equiv -1 \pmod{p}.$$

So ist z. B.

$$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 + 1 = 721$$

theilbar durch 7.

Der Wilson'sche Satz gilt aber auch für die Primzahl 2, da in diesem Fall $+1$ und -1 einander congruent sind.

Dieser Satz ist dadurch bemerkenswerth, dass er sich umkehren lässt und deshalb ein charakteristisches Merkmal für eine Primzahl abgiebt. Denn nimmt man umgekehrt an, es sei

$$1 \cdot 2 \cdot 3 \cdots (p-1) + 1$$

durch p theilbar, so muss p eine Primzahl sein; wäre nämlich p eine zusammengesetzte Zahl, also ausser durch 1 und durch sich selbst auch noch durch eine andere Zahl a theilbar, so würde a nothwendig eine der Zahlen $2, 3 \ldots (p-1)$ sein müssen; da nun die obige Summe und ihr erstes Glied durch a theilbar ist, so müsste auch das zweite Glied 1 durch a theilbar sein, was nicht möglich ist.

Einen andern interessanten Satz erhält man durch Anwendung des dritten der vorhergehenden Sätze auf dasselbe Beispiel. Bezeichnet nämlich δ irgend einen Divisor von $p-1$, so ist bekanntlich

$$x^{p-1} - 1 = (x^{\delta} - 1)\, \psi(x),$$

wo $\psi(x)$ ein Polynom mit ganzen Coefficienten bedeutet. Hieraus folgt also, dass die Congruenz

$$x^{\delta} \equiv 1 \pmod{p},$$

deren Grad δ ein Divisor von $p-1$ ist, stets δ incongruente Wurzeln besitzt.

§. 28.

Der zuletzt abgeleitete Satz gehört seinem Inhalte nach eigentlich in eine allgemeinere Theorie, nämlich in die Theorie der *binomischen Congruenzen* von der Form

$$a x^n \equiv b \text{ (mod. } k).$$

Dieselbe stützt sich auf die Betrachtung der sogenannten *Potenzreste*, d. h. der Reste der successiven Potenzen einer Zahl, und wir beschäftigen uns daher zunächst mit der Untersuchung der interessanten Gesetze, welche hier hervortreten.

Es sei also k ein beliebiger Modul, und a relative Primzahl gegen denselben; bilden wir nun die Reihe

$$1, a, a^2, a^3 \ldots$$

der successiven Potenzen von a und setzen dieselbe hinreichend weit fort, so muss es einmal geschehen, dass zwei verschiedene Glieder a^s und a^{s+n} einander nach dem Modul k congruent werden; denn es giebt ja nur eine endliche Anzahl incongruenter Zahlen. Aus der Congruenz

$$a^{s+n} = a^s \cdot a^n \equiv a^s \text{ (mod. } k)$$

folgt aber, da a^s relative Primzahl gegen den Modul k ist, dass

$$a^n \equiv 1 \text{ (mod. } k)$$

ist. Es giebt daher, was wir auch schon durch den verallgemeinerten Fermat'schen Satz (§. 19) wussten, stets eine Potenz von a, welche durch k dividirt den Rest 1 lässt. Unter allen Potenzen von a, welche dieselbe Eigenschaft haben, ist aber besonders diejenige bemerkenswerth, welche den kleinsten Exponenten hat; doch versteht sich von selbst, dass der Exponent Null hier nicht in Betracht kommt, für welchen die entsprechende Potenz ja stets $\equiv 1$ sein würde. Bezeichnen wir mit δ diesen kleinsten positiven Exponenten, für welchen

$$a^\delta \equiv 1 \text{ (mod. } k)$$

wird, so wollen wir sagen, die Zahl a *gehöre* zu dem Exponenten δ oder zu der Zahl δ. Dann leuchtet zunächst ein, dass die ersten δ Glieder der obigen Potenzreihe, d. h. die Zahlen

$$1,\ a,\ a^2 \dots a^{\delta-1}$$

sämmtlich incongruent unter einander sind; denn aus einer Congruenz von der Form $a^{s+n} \equiv a^s$, wo s und $s+n$ kleiner als δ sind, würde wieder $a^n \equiv 1$ folgen, was mit der Voraussetzung im Widerspruch steht, dass keine niedrigere Potenz als a^δ den Rest 1 lässt.

Die folgenden Glieder der Reihe geben nun genau dieselben Reste, und auch in derselben Reihenfolge, denn es ist

$$a^\delta \equiv 1,\ a^{\delta+1} \equiv a,\ a^{\delta+2} \equiv a^2 \dots a^{2\delta-1} \equiv a^{\delta-1}$$
$$a^{2\delta} \equiv 1,\ a^{2\delta+1} \equiv a,\ a^{2\delta+2} \equiv a^2 \dots a^{3\delta-1} \equiv a^{\delta-1}$$
$$a^{3\delta} \equiv 1,\ a^{3\delta+1} \equiv a,\ a^{3\delta+2} \equiv a^3 \dots a^{4\delta-1} \equiv a^{\delta-1}$$

u. s. w.

Um daher zu erfahren, welchen Rest eine beliebige Potenz a^s lässt, dividire man den Exponenten s durch δ und bringe dadurch s in die Form $s = m\delta + r$, wo r eine der Zahlen 0, 1, 2... $(\delta - 1)$ bezeichnet. Dann ist

$$a^s = a^{m\delta+r} \equiv a^r \text{ (mod. } k).$$

Hieraus geht ferner hervor, dass zwei solche Potenzen a^s und $a^{s'}$ stets, aber auch nur dann congruent sein werden in Bezug auf den Modul k, wenn $s \equiv s'$ (mod. δ); denn ist r' der bei der Division von s' durch δ hervorgehende Rest, so ist $a^{s'} \equiv a^{r'}$ (mod. k). Ist daher

$$a^s \equiv a^{s'} \text{ (mod. } k)$$

so muss auch

$$a^r \equiv a^{r'} \text{ (mod. } k)$$

sein; da aber r und r' kleiner als δ sind, so ist dies nur dann möglich, wenn $r = r'$ ist, woraus $s \equiv s'$ (mod. δ) folgt; und um-

gekehrt leuchtet ein, dass, sobald $s \equiv s'$ (mod. δ), also $r = r'$ ist, auch $a^s \equiv a^{s'}$ (mod. k) sein muss.

Ein specieller Fall ist der, dass, sobald $a^s \equiv 1$, also $a^s \equiv a^0$ ist, nothwendig $s \equiv 0$ (mod. δ), d. h. dass s theilbar durch δ sein muss. Nun wissen wir schon aus dem verallgemeinerten Fermat'schen Satz, dass stets

$$a^{\varphi(k)} \equiv 1 \text{ (mod. } k)$$

ist; hieraus folgt also, dass die Zahl δ, zu welcher eine Zahl a gehört, stets ein Divisor von $\varphi(k)$ sein muss*).

§. 29.

Beschränken wir uns jetzt wieder auf den Fall, in welchem der Modul eine Primzahl p, und also a irgend eine durch p nicht theilbare Zahl ist, so folgt aus der letzten Bemerkung, dass die Zahl δ, zu welcher a gehört, jedenfalls ein Divisor von $\varphi(p) = p - 1$ sein muss. Man kann nun umgekehrt fragen: wenn δ irgend ein Divisor von $p - 1$ ist, giebt es dann jedesmal auch Zahlen a, welche zu δ gehören? und wie viele? Nehmen wir zunächst einmal ein Beispiel, indem wir $p = 7$ setzen. Da aus $a \equiv a'$ (mod. p) auch stets $a^s \equiv a'^s$ (mod. p) folgt, so gehören je zwei congruente Zahlen auch stets zu demselben Exponenten, und wir brauchen daher in unserm Beispiel nur die Zahlen $a = 1, 2, 3, 4, 5, 6$ zu betrachten; durch wirkliches Potenziren, welches man dadurch abkürzt, dass man statt jeder Potenz immer ihren kleinsten Rest substituirt, findet man nun das in der folgenden Tabelle ausgedrückte Resultat:

a	1	2	3	4	5	6
δ	1	3	6	3	6	2

Es gehört daher zu dem Divisor $\delta = 1$ nur die einzige Zahl 1, zu $\delta = 2$ nur die einzige Zahl 6; zu $\delta = 3$ gehören zwei Zahlen, nämlich 2 und 4, und zu $\delta = 6$ gehören die beiden Zahlen 3 und 5.

*) Ein anderer Beweis dieses Satzes findet sich in den Supplementen V. §. 127.

Nehmen wir nun vorläufig einmal an, dass *mindestens eine* Zahl a existirt, welche zu dem Exponenten δ gehört, so sind die δ Zahlen

$$1,\ a,\ a^2\ \ldots\ a^{\delta-1} \qquad (A)$$

nach dem Vorhergehenden sämmtlich incongruent; da ferner $a^\delta \equiv 1$, so ist auch

$$(a^r)^\delta = (a^\delta)^r \equiv 1 \pmod{p},$$

d. h. die δ Zahlen (A) sind Wurzeln der Congruenz

$$x^\delta \equiv 1 \pmod{p},$$

und da sie unter einander incongruent sind, und der Modulus eine Primzahl ist, so bilden sie auch die sämmtlichen Wurzeln dieser Congruenz vom Grade δ. Jede Zahl aber, welche zum Exponenten δ gehört, muss vor Allem eine Wurzel dieser Congruenz sein, und wir haben daher alle etwa existirenden Zahlen, die zu δ gehören, unter den Zahlen (A) zu suchen. Wir fragen daher: zu welchem Exponenten h gehört irgend eine dieser Zahlen, z. B. a^r? d. h. welches ist die kleinste positive Zahl h, für welche

$$(a^r)^h = a^{rh} \equiv 1 \pmod{p}$$

ist? Offenbar muss rh (da a zum Exponenten δ gehört) durch δ theilbar sein; ist daher ε der grösste gemeinschaftliche Divisor von r und δ, so muss h durch $\frac{\delta}{\varepsilon}$ theilbar sein, und die kleinste Zahl h, welche diese Bedingung erfüllt, ist offenbar $\frac{\delta}{\varepsilon}$, und dann ist auch wirklich

$$(a^r)^h = (a^\delta)^{\frac{r}{\varepsilon}} \equiv 1 \pmod{p};$$

also ist $\frac{\delta}{\varepsilon}$ die Zahl, zu welcher a^r gehört. Soll also a^r zum Exponenten δ gehören, so muss $\varepsilon = 1$, also r relative Primzahl gegen δ sein; und umgekehrt, sobald dies der Fall, also $\varepsilon = 1$ ist, gehört auch a^r wirklich zum Exponenten δ. Wir erhalten so das Resultat, dass unter den Zahlen (A) genau ebenso viele zu dem Exponenten δ gehören, als es unter den Exponenten

$$0, 1, 2 \ldots (\delta - 1)$$

relative Primzahlen zu δ giebt; es giebt daher $\varphi(\delta)$ solche Zahlen.

Da wir angenommen hatten, dass *mindestens eine* solche Zahl a existirte, so können wir das Bisherige so zusammenfassen: Ist p eine Primzahl und δ ein Divisor von $p - 1$, so ist die Anzahl der incongruenten Zahlen, die zu δ gehören, entweder $= 0$, oder $= \varphi(\delta)$. Um nun über diese Alternative zu entscheiden, betrachten wir die Totalität aller $p - 1$ nach dem Modul p incongruenten und durch p nicht theilbaren Zahlen; wir theilen dieselben in Gruppen ein, indem wir je zwei incongruente Zahlen in dieselbe oder in verschiedene Gruppen werfen, je nachdem sie zu demselben Divisor δ von $p - 1$ gehören oder zu verschiedenen. Bezeichnen wir mit $\psi(\delta)$ die Anzahl der Individuen, welche in die dem Divisor δ entsprechende Gruppe gehören, so muss, da jede der $p - 1$ vertheilten Zahlen in eine, aber auch nur in eine solche Gruppe gehört,

$$\Sigma\, \psi(\delta) = p - 1$$

sein, wo sich das Summenzeichen auf sämmtliche Divisoren δ von $p - 1$ bezieht; wir wissen ferner schon, dass

$$\psi(\delta) \text{ entweder } = 0, \text{ oder } = \varphi(\delta)$$

ist. Da nun früher bewiesen ist (§. 13), dass auch

$$\Sigma\, \varphi(\delta) = p - 1$$

ist, so folgt hieraus mit Nothwendigkeit, dass

$$\psi(\delta) \text{ niemals } = 0, \text{ sondern stets } = \varphi(\delta)$$

ist. Denn da jedes Glied $\psi(\delta)$ der erstern Summe dem entsprechenden der letztern höchstens gleich sein, aber niemals dasselbe übertreffen kann, so würde, sobald nur ein einziges Mal oder öfter $\psi(\delta) = 0$ wäre, die erstere Summe nothwendig kleiner ausfallen müssen, als die letztere, während sie in der That einander gleich sind. Wir haben so den wichtigen Satz gewonnen:

Die Anzahl der sämmtlichen incongruenten Zahlen, welche zu einem bestimmten Divisor δ von $p - 1$ gehören ist stets $= \varphi(\delta)$.

Es genügt, einen Blick auf das obige Beispiel zu werfen, in welchem $p = 7$, um diesen Satz bestätigt zu sehen.

§. 30.

Am interessantesten und folgenreichsten ist der in diesem Resultat enthaltene specielle Fall, in welchem $\delta = p - 1$ ist:

Es giebt stets $\varphi(p-1)$ incongruente Zahlen g, welche zu dem Exponenten $p-1$ gehören, welche also die charakteristische Eigenschaft haben, dass die $p-1$ Potenzen

$$1,\ g,\ g^2,\ g^3\ \ldots\ g^{p-2} \qquad (G)$$

sämmtlich incongruent (mod. p) sind.

Da es überhaupt nur $p-1$ incongruente und durch p nicht theilbare Zahlen c giebt, so folgt, dass jede solche Zahl c einer, und natürlich auch nur einer der Potenzen (G) congruent ist. Jede solche Zahl g, welche zum Exponenten $p-1$ gehört, heisst eine *primitive Wurzel der Primzahl* p, und man kann daher sagen: wenn g eine primitive Wurzel von p ist, und c irgend eine durch p nicht theilbare Zahl, so existirt stets eine Zahl γ in der Reihe $0, 1, 2 \ldots p-2$ und nur eine von der Beschaffenheit, dass

$$c \equiv g^\gamma \pmod{p}$$

ist. Wenn man in dieser Weise alle incongruenten und — was im Folgenden immer hinzuzudenken ist — durch p nicht theilbaren Zahlen als Potenzen einer Basis g darstellt, so heissen die Exponenten γ die *Indices* der zugehörigen Zahlen c in Bezug auf die *Basis* g, und man schreibt z. B.

$$\text{Ind. } c = \gamma,$$

indem man die Basis g, so lange sie unverändert bleibt, in der Bezeichnung unterdrückt.

Nehmen wir z. B. $p = 13$, so überzeugt man sich leicht, dass 2 eine primitive Wurzel ist; denn durch Potenziren erhält man

$$2^0 \equiv 1,\ 2^1 \equiv 2,\ 2^2 \equiv 4,\ 2^3 \equiv 8,\ 2^4 \equiv 3,\ 2^5 \equiv 6,$$

$$2^6 \equiv 12,\ 2^7 \equiv 11,\ 2^8 \equiv 9,\ 2^9 \equiv 5,\ 2^{10} \equiv 10,\ 2^{11} \equiv 7.$$

Nehmen wir daher 2 zur Basis eines Systems von Indices, so erhalten wir folgende Tabellen

c	1	2	3	4	5	6	7	8	9	10	11	12
Ind. c	0	1	4	2	9	5	11	3	8	10	7	6

und

Ind. c	0	1	2	3	4	5	6	7	8	9	10	11
c	1	2	4	8	3	6	12	11	9	5	10	7

deren erstere dazu dient, zu einer Zahl c den Index zu finden, während die zweite den entgegengesetzten Zweck hat *).

Offenbar hat dieses ganze Verfahren die grösste Analogie mit der Construction von Logarithmentafeln, die ja auf dem ähnlichen Gedanken beruhen, alle positiven Zahlen als Potenzen einer einzigen Basis darzustellen; und es zeigt sich nun auch, dass in der Zahlentheorie die Indices ähnliche Gesetze befolgen und für praktische Zwecke ebenso brauchbar sind, wie die Logarithmen. Zunächst leuchtet ein, dass zwei congruente Zahlen auch stets denselben Index haben, in Zeichen: wenn $a \equiv b \pmod{p}$, so ist auch Ind. $a =$ Ind. b. Ist ferner $c \equiv a\,b \pmod{p}$, so ist Ind. $c \equiv$ Ind. $a +$ Ind. $b \pmod{p - 1}$, oder kürzer, es ist stets

$$\text{Ind.}\,(ab) \equiv \text{Ind.}\,a + \text{Ind.}\,b \pmod{p-1}.$$

Denn es ist ja

$$a \equiv g^{\text{Ind.}\,a} \pmod{p};\ b \equiv g^{\text{Ind.}\,b} \pmod{p},$$

also

$$ab \equiv g^{\text{Ind.}\,a\,+\,\text{Ind.}\,b} \pmod{p};$$

nun ist aber auch

$$ab \equiv g^{\text{Ind.}\,(ab)} \pmod{p},$$

folglich

$$g^{\text{Ind.}\,(ab)} \equiv g^{\text{Ind.}\,a\,+\,\text{Ind.}\,b} \pmod{p}.$$

Da nun g eine primitive Wurzel von p, also eine zum Exponenten $\delta = (p - 1)$ gehörende Zahl ist, so folgt aus §. 28 die Richtigkeit der zu beweisenden Congruenz nach dem Modul $p - 1$. Nehmen wir unser obiges Beispiel, in welchem $p = 13$, so ist z. B.

$$\text{Ind.}\,(7) = 11,\ \text{Ind.}\,(9) = 8,$$

*) Im *Canon Arithmeticus* von *Jacobi* (1839) findet man solche Tabellen für alle dem ersten Tausend angehörenden Primzahlen.

folglich

$$\text{Ind. } (63) \equiv 19 \pmod{12}$$

oder

$$\text{Ind. } (63) = 7.$$

In der That ist aber $63 \equiv 11 \pmod{13}$, und Ind. $(11) = 7$. Man sieht aus diesem Beispiel, wie eine solche Doppeltafel der Indices dazu benutzt werden kann, mit Leichtigkeit die Classe (11) zu finden, welcher das Product (63) aus zwei Zahlen (7 und 9) angehört.

Natürlich lässt sich der vorstehende Satz auf ein Product aus beliebig vielen Factoren in folgender Weise ausdehnen:

$$\text{Ind. } (abc \cdots) \equiv \text{Ind. } a + \text{Ind. } b + \text{Ind. } c + \cdots \pmod{p - 1}.$$

Nimmt man hierin alle Factoren einander congruent, so erhält man:

$$\text{Ind. } (a^n) \equiv n \text{ Ind. } a \pmod{p - 1},$$

wo n irgend eine positive ganze Zahl bedeutet.

Es liesse sich hieraus auch leicht nachweisen, dass der Uebergang von einem System von Indices zu einem andern, dessen Basis eine andere der $\varphi(p - 1)$ primitiven Wurzeln ist, ganz ähnlichen Gesetzen unterliegt, wie der Uebergang von einem Logarithmensystem zu einem andern; wir beschränken uns indessen auf folgende einfache Bemerkungen. Wie auch die Basis g gewählt sein mag, der Index von 1 ist stets $= 0$; denn es ist immer $g^0 = 1$. Ferner ist (den Fall $p = 2$ ausgenommen) der Index von -1 stets $= \frac{1}{2}(p - 1)$; denn da nach §. 19

$$g^{p-1} - 1 = \left(g^{\frac{p-1}{2}} - 1\right)\left(g^{\frac{p-1}{2}} + 1\right) \equiv 0 \pmod{p}$$

ist, so muss mindestens eine der beiden Zahlen

$$g^{\frac{p-1}{2}} - 1, \quad g^{\frac{p-1}{2}} + 1$$

durch p theilbar sein; die erstere ist es aber nicht, denn sonst wäre

$$g^{\frac{p-1}{2}} \equiv 1 \pmod{p},$$

was mit der Voraussetzung im Widerspruch ist, dass g zum Exponenten $p - 1$ gehört; es ist daher stets

$$g^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

und folglich

$$\text{Ind.}\,(-1) = \frac{p-1}{2}.$$

Es verdient endlich noch bemerkt zu werden, dass man die Indices, statt aus den Zahlen 0, 1, 2 . . . $(p-2)$, ebenso gut aus jedem andern vollständigen System incongruenter Zahlen in Bezug auf den Modul $p-1$ wählen kann; die so eben bewiesenen Fundamentalsätze erleiden dadurch nicht die geringste Aenderung.

Man kann nun die Indices benutzen, um eine Congruenz ersten Grades

$$ax \equiv b \pmod{p},$$

die hier die Stelle eines Divisionsproblems vertritt, mit Leichtigkeit aufzulösen; denn es muss offenbar

$$\text{Ind.}\,x \equiv \text{Ind.}\,b - \text{Ind.}\,a \pmod{p-1}$$

sein. Ist also z. B. die Congruenz

$$5x \equiv 6 \pmod{13}$$

zu lösen, so wird man, indem man wieder die primitive Wurzel 2 zur Basis des Indexsystemes wählt,

$$\text{Ind.}\,x \equiv \text{Ind.}\,6 - \text{Ind.}\,5 \equiv 5 - 9 \equiv 8 \pmod{12}$$

und folglich

$$x \equiv 9 \pmod{13}$$

finden.

Diese Methode, Congruenzen ersten Grades aufzulösen, scheint auf den ersten Blick nur dann anwendbar, wenn der Modul eine Primzahl ist; allein man kann leicht zeigen, dass jede beliebige Congruenz ersten Grades

$$ax \equiv b \pmod{k},$$

deren Modul eine zusammengesetzte Zahl ist, auf eine Kette von Congruenzen reducirt werden kann, deren Moduln Primzahlen sind. Wir können uns hierbei auf den Fall beschränken, in welchem a relative Primzahl gegen k ist. Man löse nun zuerst die Congruenz

$$ax \equiv b \pmod{p},$$

wo p irgend eine in $k = pk'$ aufgehende Primzahl ist, nach der neuen Methode, so erhält man ein Resultat von der Form

$$x \equiv \alpha \text{ (mod. } p) \quad \text{oder} \quad x = \alpha + px',$$

wo x' eine beliebige ganze Zahl ist; substituirt man diesen Ausdruck in die gegebene Congruenz, so nimmt sie die folgende Form an:

$$pax' \equiv b - a\alpha \text{ (mod. } k).$$

Da nun $b - a\alpha$ durch p theilbar, also von der Form $b'p$ ist, so stimmen sämmtliche Wurzeln der vorstehenden Congruenz mit den sämmtlichen Wurzeln der Congruenz

$$ax' \equiv b' \text{ (mod. } k')$$

überein. Auf dieselbe Weise kann man nun fortfahren, indem man diese Congruenz zunächst nur in Bezug auf eine in k' aufgehende Primzahl p' löst, u. s. f.; man braucht dann zuletzt nur noch von der Wurzel der letzten dieser Congruenzen durch successive Substitution zu der der ursprünglichen überzugehen.

§. 31.

Wir benutzen nun noch die Theorie der Indices, um auf sie die Theorie der *binomischen Congruenzen* für einen Primzahl-Modulus p zu stützen; nach einer frühern Bemerkung kann man einer jeden solchen binomischen Congruenz die Form

$$x^n \equiv D \text{ (mod. } p) \tag{1}$$

geben, in welcher der Coefficient der Potenz der Unbekannten $= 1$ ist; da ferner der Fall, in welchem $D \equiv 0$ (mod. p) und folglich auch $x \equiv 0$ (mod. p), ohne Interesse ist, so schliessen wir denselben aus.

Bezeichnen wir nun zur Abkürzung die Indices von D und x resp. mit γ und ξ (wenn irgend eine primitive Wurzel g von p zur Basis genommen ist), so reducirt sich die Auflösung der Congruenz (1) auf die Bestimmung aller Wurzeln ξ der Congruenz ersten Grades

$$n\xi \equiv \gamma \text{ (mod. } p - 1); \tag{2}$$

denn offenbar entspricht jeder Wurzel der einen dieser beiden Congruenzen (1) und (2) auch stets eine und nur eine Wurzel der andern.

Es sei jetzt δ der grösste gemeinschaftliche Divisor der Zahlen $p - 1$ und n, so ist (§. 22) die Congruenz (2) nur dann möglich, wenn die Bedingung

$$\gamma \equiv 0 \pmod{\delta} \qquad (3)$$

erfüllt ist, und dann hat sie δ nach dem Modul $p - 1$ incongruente Wurzeln ξ. Wir schliessen hieraus unmittelbar den Satz:

Ist δ der grösste gemeinschaftliche Divisor des Grades n der Congruenz (1) *und der Zahl $p - 1$, so ist diese Congruenz nur dann möglich, wenn die Bedingung*

$$\text{Ind. } D \equiv 0 \pmod{\delta} \qquad (4)$$

erfüllt ist, und dann besitzt sie δ nach dem Modul p incongruente Wurzeln x.

Liegt z. B. die Congruenz

$$x^8 \equiv 3 \pmod{13}$$

vor, so ist $\delta = 4$; nehmen wir ferner die primitive Wurzel 2 als Basis für die Indices, so ist Ind. $3 = 4$, also ist die Bedingung (4) erfüllt, und die vorgelegte Congruenz hat 4 nach dem Modul 13 incongruente Wurzeln; um diese zu finden, bilden wir die Congruenz ersten Grades

$$8\xi \equiv 4 \pmod{12} \text{ oder } 2\xi \equiv 1 \pmod{3},$$

und erhalten hieraus

$$\xi \equiv 2 \pmod{3}$$

oder

$$\xi \equiv 2, \text{ oder } 5, \text{ oder } 8, \text{ oder } 11 \pmod{12},$$

folglich, indem wir zu diesen Indices ξ die zugehörigen Zahlen suchen,

$$x \equiv 4, \text{ oder } 6, \text{ oder } 9, \text{ oder } 7 \pmod{13}.$$

Da die Möglichkeit der binomischen Congruenz von der Wahl der primitiven Wurzel g, auf welche sich die Indices γ und ξ beziehen, nothwendig unabhängig sein muss, so wird das Kriterium, dass der Index γ einer Zahl D durch einen Divisor δ der Zahl $p - 1$ theilbar sein muss, in eine von der Theorie der Indices unabhängige Form gebracht werden können. Dies bestätigt sich auf folgende Weise. Sobald in Bezug auf irgend eine Basis g der Index γ der Zahl D durch den Divisor δ von $p - 1$ theilbar, also von der Form $h\delta$ ist, so haben wir die Congruenz

$$D \equiv g^{h\delta} \pmod{p};$$

erhebt man dieselbe zur $\left(\frac{p-1}{\delta}\right)$ten Potenz, so ergiebt sich

$$D^{\frac{p-1}{\delta}} \equiv g^{h(p-1)} \equiv 1 \pmod{p};$$

und umgekehrt, sobald die Zahl D dieser Bedingung

$$D^{\frac{p-1}{\delta}} \equiv 1 \pmod{p}$$

genügt, muss der in Bezug auf eine beliebige Basis g genommene Index γ der Zahl D durch δ theilbar sein; denn es sei

$$D \equiv g^{\gamma} \pmod{p},$$

so folgt hieraus

$$g^{\gamma \cdot \frac{p-1}{\delta}} \equiv 1 \pmod{p},$$

und da g eine primitive Wurzel, d. h. eine zum Exponenten $p-1$ gehörende Zahl ist, so muss $\gamma \cdot \frac{p-1}{\delta}$ durch $p-1$, und folglich der Index γ durch δ theilbar sein.

Nachdem das ursprüngliche Kriterium so umgeformt ist, können wir unsern Satz in folgender Weise unabhängig von der Theorie der Indices aussprechen:

Ist δ der grösste gemeinschaftliche Divisor der Zahlen n und $p-1$, so hat die Congruenz

$$x^n \equiv D \pmod{p}, \tag{1}$$

genau δ incongruente Wurzeln, oder gar keine, je nachdem die Zahl D der Bedingung

$$D^{\frac{p-1}{\delta}} \equiv 1 \pmod{p} \tag{5}$$

genügt oder nicht genügt.

Den speciellen Fall, in welchem $\delta = n$ und $D = 1$ ist, haben wir schon früher (§. 27) auf anderm Wege bewiesen; es würde nicht schwer sein, aus den dort angewandten Principien auch den allgemeinen Satz abzuleiten, ohne die Theorie der Indices zu Hülfe zu rufen; doch überlassen wir der Kürze halber diese Untersuchung dem Leser.

Wir können nun auch noch die Frage aufstellen: wenn der Grad n der Congruenz (1) gegeben ist, wie viele incongruente Zahlen D existiren, für welche die Congruenz (1) möglich ist?

Hierauf liefert der Satz selbst sogleich die Antwort, denn diese Zahlen D sind ja die sämmtlichen Wurzeln der binomischen Congruenz

$$x^{\frac{p-1}{\delta}} \equiv 1 \pmod{p};$$

der grösste gemeinschaftliche Divisor des Exponenten $\frac{p-1}{\delta}$ und der Zahl $p - 1$ ist in diesem Fall der Exponent $\frac{p-1}{\delta}$ selbst, und da das Kriterium für die Möglichkeit offenbar erfüllt ist, so ist also die Anzahl aller incongruenten Zahlen D, für welche die Congruenz (1) möglich ist, genau $= \frac{p-1}{\delta}$. Man nennt solche Zahlen D, welche einer $n$ten Potenz einer Zahl congruent sind, kurz $n$te Potenzreste, und wir können daher sagen: die Anzahl aller $n$ten Potenzreste ist $= \frac{p-1}{\delta}$, wo δ den grössten gemeinschaftlichen Divisor der Zahlen n und $p - 1$ bezeichnet. Man findet dieselben offenbar, wenn man alle incongruenten Zahlen zur $n$ten Potenz erhebt und deren Reste bildet. Wenn $n =$ 2, 3, 4 ist, so nennt man diese Zahlen resp. *quadratische*, *cubische*, *biquadratische Reste*. Mit der Theorie der erstern, welche für sich allein schon eine grosse Ausdehnung besitzt, werden wir uns nun im Folgenden ausführlich beschäftigen.

Dritter Abschnitt.

Von den quadratischen Resten.

§. 32.

Wir betrachten im Folgenden ausführlich die Theorie der Congruenzen von der Form

$$x^2 \equiv D \pmod{k}, \qquad (1)$$

in welcher wir stets D als *relative Primzahl* gegen den Modul k voraussetzen. Es würde sich leicht zeigen lassen, dass jede beliebige Congruenz zweiten Grades auf diesen Fall zurückgeführt werden kann; doch wollen wir uns dabei nicht aufhalten. So oft nun die Congruenz (1) möglich ist, d. h. so oft sie Wurzeln hat, heisst die Zahl D *quadratischer Rest der Zahl* k; im entgegengesetzten Fall heisst D *quadratischer Nichtrest der Zahl* k. Man lässt auch häufig, wenn kein Missverständniss zu befürchten ist, das Beiwort „quadratisch" fort und nennt kurz die Zahl D *Rest* oder *Nichtrest* von k, je nachdem die Congruenz (1) möglich ist oder nicht. Unmittelbar leuchtet hieraus ein, dass zwei nach dem Modul k congruente Zahlen entweder beide Reste von k, oder beide Nichtreste von k sind; d. h. alle in einer und derselben *Classe* enthaltenen Zahlen haben denselben Charakter; je nachdem eine von ihnen Rest oder Nichtrest des Modul k ist, sind sie alle Reste oder alle Nichtreste von k.

Die Theorie der quadratischen Reste zerfällt nun in zwei Haupttheile; man kann nämlich einmal die Frage aufwerfen:

Wenn der Modul k gegeben ist, welches sind dann die sämmtlichen incongruenten quadratischen Reste von k? und wie viele Wurzeln hat die einer jeden dieser Zahlen entsprechende Congruenz?

Bei weitem schwieriger ist aber die Beantwortung der folgenden zweiten Hauptfrage:

Wenn die Zahl D gegeben ist, welches sind dann die Moduln k, für welche die Congruenz (1) *möglich ist, d. h. welches sind die Zahlen k, von denen die gegebene Zahl D quadratischer Rest ist?*

§. 33.

Wir beschäftigen uns zuerst mit der ersten Frage und beginnen die Untersuchung mit dem einfachsten Fall, mit dem nämlich, wo der Modul eine *ungerade Primzahl* p ist (der Fall $p = 2$ erledigt sich unmittelbar durch die Bemerkung, dass jede ungerade Zahl $\equiv 1^2$, also quadratischer Rest von 2 ist). Hier erhalten wir die vollständige Antwort sogleich durch die vorhergehende Theorie der binomischen Congruenzen (§. 31). In unserm Fall ist nämlich $n = 2$ der Grad der binomischen Congruenz, und da $p - 1$ gerade ist, so ist $\delta = 2$ der grösste gemeinschaftliche Divisor von n und $p - 1$; die Congruenz

$$x^2 \equiv D \pmod{p}$$

ist daher stets und nur dann möglich, wenn

$$D^{\frac{p-1}{2}} \equiv 1 \pmod{p},$$

und zwar hat sie jedesmal zwei incongruente Wurzeln; es giebt $\frac{1}{2}(p-1)$ quadratische Reste, und folglich, da die Anzahl aller incongruenten und durch p nicht theilbaren Zahlen gleich $p - 1$ ist, auch $\frac{1}{2}(p-1)$ Nichtreste von p. Da ferner nach dem Fermat'schen Satze

$$D^{p-1} - 1 = (D^{\frac{p-1}{2}} - 1)(D^{\frac{p-1}{2}} + 1) \equiv 0 \pmod{p}$$

ist, so folgt, dass

$$D^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

sein muss, so oft D ein Nichtrest von p ist. Je nachdem also

$D^{\frac{p-1}{2}} \equiv +1$ oder $\equiv -1$ ist, ist D ein Rest oder Nichtrest von p. Nennt man die Eigenschaft einer Zahl D, Rest oder Nichtrest von p zu sein, ihren *Charakter*, so ist derselbe also durch dieses Kriterium vollständig bestimmt.

Es lässt sich indessen auch ganz elementar beweisen, dass die Anzahl sowohl der Reste als auch der Nichtreste $= \frac{1}{2}(p-1)$ ist. Quadrirt man nämlich die $\frac{1}{2}(p-1)$ Zahlen

$$1,\ 2,\ 3\ \ldots\ \frac{p-1}{2},$$

so sind die Quadrate sämmtlich incongruent; denn sind r und s zwei verschiedene dieser Zahlen, so ist die Differenz ihrer Quadrate

$$r^2 - s^2 = (r+s)(r-s)$$

nicht theilbar durch p, da die Factoren $r+s$ und $r-s$ kleiner als p sind. Diese $\frac{1}{2}(p-1)$ Quadrate geben also wirklich $\frac{1}{2}(p-1)$ incongruente quadratische Reste; dagegen liefern die Quadrate der folgenden Zahlen

$$\frac{p+1}{2},\ \frac{p+3}{2}\ \ldots\ (p-1)$$

dieselben Reste wieder; denn es ist allgemein

$$(p-r)^2 = p^2 - 2rp + r^2 \equiv r^2 \pmod{p}.$$

Also ist $\frac{1}{2}(p-1)$ die Anzahl aller quadratischen Reste, und folglich auch die der quadratischen Nichtreste.

Da ein Product aus mehreren Factoren, die nicht durch p theilbar sind, dieselbe Eigenschaft hat, so kann man nach dem Charakter des Productes fragen, wenn die Charaktere der Factoren gegeben sind. Beschränken wir uns zunächst auf zwei Factoren, so sind folgende drei Fälle zu unterscheiden.

I. Das Product aus zwei Resten ist wieder ein Rest; denn sind a und a' Reste, so giebt es Zahlen x, x' von der Beschaffenheit, dass

$$a \equiv x^2 \pmod{p},\ \ a' \equiv x'^2 \pmod{p};$$

hieraus folgt aber

$$aa' \equiv (xx')^2 \pmod{p},$$

d. h. aa' ist Rest von p.

II. Das Product aus einem Rest und einem Nichtrest ist ein Nichtrest. Denn wenn wir ein vollständiges System incongruenter und durch p nicht theilbarer Zahlen bilden, so zerfällt dasselbe in zwei Gruppen, deren eine $\frac{1}{2}(p-1)$ Reste — wir wollen sie allgemein mit α bezeichnen — und deren zweite $\frac{1}{2}(p-1)$ Nichtreste β enthält. Multiplicirt man nun alle diese Zahlen α und β mit einem Reste a, so bilden die Producte $a\alpha$ und $a\beta$ wieder ein vollständiges System incongruenter (durch p nicht theilbarer) Zahlen, welches also wieder $\frac{1}{2}(p-1)$ Reste und $\frac{1}{2}(p-1)$ Nichtreste enthält. In der That sind nun (nach I) die Producte $a\alpha$ sämmtlich wieder Reste; es müssen daher die andern $\frac{1}{2}(p-1)$ Producte $a\beta$ sämmtlich Nichtreste sein; also ist das Product aus jedem Rest a und jedem Nichtrest β ein Nichtrest.

III. Das Product aus zwei Nichtresten ist ein Rest. Denn bildet man wieder das System der Reste α und Nichtreste β, und multiplicirt dieselben mit einem Nichtreste b, so sind die Producte $b\alpha$ (nach II) sämmtlich Nichtreste; folglich müssen die übrigen $\frac{1}{2}(p-1)$ Producte $b\beta$ sämmtlich Reste sein.

Man kann diese wichtigen Sätze offenbar in den folgenden einen zusammenfassen:

Ein Product aus beliebig vielen durch die Primzahl p nicht theilbaren Zahlen ist Rest oder Nichtrest von p, je nachdem die Anzahl der Nichtreste, welche sich unter den Factoren finden, gerade oder ungerade ist.

Dieser Satz ergiebt sich auch unmittelbar aus dem oben aufgestellten Kriterium für den Charakter einer Zahl; denn da

$$(abc\cdots)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}}\, b^{\frac{p-1}{2}}\, c^{\frac{p-1}{2}} \cdots$$

so wird

$$(abc\cdots)^{\frac{p-1}{2}} \equiv +1 \quad \text{oder} \quad \equiv -1 \pmod{p}$$

sein, je nachdem die Anzahl der Factoren $a^{\frac{p-1}{2}}, b^{\frac{p-1}{2}}, c^{\frac{p-1}{2}}\ldots,$ welche $\equiv -1$ sind, eine gerade oder ungerade ist.

Man kann diesen Satz in Form einer Gleichung ausdrücken, wenn man sich eines von *Legendre* in die Zahlentheorie eingeführten Zeichens bedient, welches in allen folgenden Untersuchungen eine grosse Rolle spielt. *Legendre* bezeichnet nämlich durch das Symbol $\left(\frac{m}{p}\right)$ die positive oder negative Einheit, je nachdem die durch die Primzahl p nicht theilbare Zahl m quadratischer Rest oder Nichtrest von p ist; es ist daher stets

$$\left(\frac{m}{p}\right)\left(\frac{m}{p}\right) = +1 \quad \text{und} \quad m^{\frac{p-1}{2}} \equiv \left(\frac{m}{p}\right) \pmod{p}.$$

Den Satz über den Charakter eines Productes kann man dann offenbar durch die folgende Gleichung ausdrücken:

$$\left(\frac{mnl\cdots}{p}\right) = \left(\frac{m}{p}\right)\left(\frac{n}{p}\right)\left(\frac{l}{p}\right)\cdots$$

Es leuchtet ferner ein, dass, sobald $m \equiv n \pmod{p}$, auch

$$\left(\frac{m}{p}\right) = \left(\frac{n}{p}\right)$$

sein wird.

§. 34.

Es ist nun interessant zu sehen, dass die soeben gewonnenen Sätze, welche zum Theil als Resultate einer ausgedehnten Theorie, wie der der binomischen Congruenzen, erscheinen, sich aus den ersten Principien auf einem ganz elementaren Wege ableiten lassen, der zugleich einen neuen Beweis des Wilson'schen und Fermat'schen Satzes liefern wird.

Es sei D irgend eine durch die Primzahl p nicht theilbare Zahl, und r irgend eine der Zahlen

$$1,\ 2,\ 3\ \ldots\ (p-1); \tag{1}$$

dann existirt in derselben Reihe stets eine und nur eine Zahl s von der Beschaffenheit, dass

$$rs \equiv D \pmod{p}$$

ist; denn diese Zahl s ist ja die Wurzel der Congruenz ersten Grades $rx \equiv D$ (mod. p); je zwei solche Zahlen r und s der Reihe (1), deren Product $\equiv D$ ist, wollen wir zusammengehörige Zahlen nennen; offenbar ist durch eine dieser beiden Zahlen die andere ebenfalls bestimmt. Identisch können diese beiden Zahlen nur dann werden, wenn die Congruenz

$$x^2 \equiv D \text{ (mod. } p) \tag{2}$$

möglich ist. Danach theilen wir unsere Untersuchung in zwei Fälle ein.

Erstens: Die Congruenz (2) ist unmöglich. — Dann sind also je zwei zusammengehörige Zahlen von einander verschieden, und da zwei solche Paare stets identisch sind, sobald sie nur eine gemeinschaftliche Zahl haben, so zerfallen die sämmtlichen $p - 1$ Zahlen (1) in $\frac{1}{2}(p - 1)$ solche Paare zusammengehöriger Zahlen, und folglich ist ihr Product

$$1 \cdot 2 \cdot 3 \cdots (p - 1) \equiv D^{\frac{p-1}{2}} \text{ (mod. } p). \tag{3}$$

Zweitens: Die Congruenz (2) ist möglich. — Dann existirt also auch in der Reihe (1) mindestens eine Zahl ϱ von der Beschaffenheit, dass $\varrho^2 \equiv D$; sehen wir zu, ob ausser ϱ in der Reihe (1) noch eine solche Zahl σ existirt; dann muss $\sigma^2 \equiv \varrho^2$, folglich $(\sigma - \varrho)(\sigma + \varrho)$ durch p theilbar sein; da wir σ verschieden von ϱ voraussetzen, so ist $\sigma - \varrho$ nicht theilbar durch p, folglich muss $\sigma + \varrho$ theilbar durch p, also $\sigma = p - \varrho$ sein; und in der That ist wirklich $(p - \varrho)^2 \equiv D$. Trennen wir nun diese beiden Zahlen ϱ und $\sigma = p - \varrho$, deren Product $\varrho\sigma \equiv -\varrho^2 \equiv -D$ ist, von den übrigen der Reihe (1), so zerfallen die letztern in $\frac{1}{2}(p - 3)$ Paare zusammengehöriger Zahlen von der Beschaffenheit, dass jedes Paar aus zwei verschiedenen Zahlen besteht. Demnach ist in diesem Fall das Product aller Zahlen der Reihe (1):

$$1 \cdot 2 \cdot 3 \cdots (p - 1) \equiv -D^{\frac{p-1}{2}} \text{ (mod. } p). \tag{4}$$

Nun giebt es aber einen Fall, in welchem die Congruenz (2) stets möglich ist, nämlich den, in welchem $D = 1 = 1^2$; wir erhalten daher zunächst aus (4) den Satz von *Wilson*:

$$1 \cdot 2 \cdot 3 \cdots (p - 1) \equiv -1 \text{ (mod. } p), \tag{5}$$

und substituiren wir dies in die Congruenzen (3) und (4), so erhalten wir das Resultat, dass

$$D^{\frac{p-1}{2}} \equiv +1 \quad \text{oder} \quad \equiv -1 \pmod{p}$$

ist, je nachdem die Congruenz (2) möglich oder nicht möglich ist. Da endlich ein dritter Fall nicht existiren kann, so erhalten wir allgemein

$$D^{p-1} = (D^{\frac{p-1}{2}})^2 \equiv (\pm 1)^2 \equiv +1 \pmod{p},$$

also den Satz von *Fermat*.

Durch diese einfache Betrachtung sind wir also sogleich bis zu denselben Sätzen in der Theorie der quadratischen Reste gelangt, welche vorher aus der allgemeinern Theorie der binomischen Congruenzen abgeleitet waren.

§. 35.

Wir wenden uns jetzt zu der Untersuchung des Falls, in welchem der Modul k der quadratischen Congruenz

$$x^2 \equiv D \pmod{k}$$

die Potenz einer Primzahl p ist; dabei müssen wir den Fall, in welchem $p = 2$, gesondert von den übrigen behandeln, in welchen p eine ungerade Primzahl ist.

Ist zunächst p eine ungerade Primzahl, und $k = p^{\pi}$, wo π irgend eine positive ganze Zahl bedeutet, und nehmen wir an, die Congruenz

$$x^2 \equiv D \pmod{p^{\pi}} \tag{1}$$

sei möglich, so überzeugt man sich leicht, dass sie im Ganzen *zwei* incongruente Wurzeln hat; denn ist α eine Wurzel, und x irgend eine, so muss

$$x^2 - \alpha^2 \equiv (x - \alpha)(x + \alpha) \equiv 0 \pmod{p^{\pi}}$$

sein; von den beiden Factoren $x - \alpha$ und $x + \alpha$ ist aber nur einer durch p theilbar; denn wären beide durch p theilbar, so wäre auch ihre Differenz 2α, und folglich auch α durch p theilbar, was nicht der Fall ist, da wir D als nicht theilbar durch p vorausgesetzt haben. Da also einer der beiden Factoren relative

Primzahl gegen p^π ist, so muss der andere für sich allein durch p^π theilbar sein. Es ist daher entweder

$$x \equiv \alpha \text{ (mod. } p^\pi), \quad \text{oder} \quad x \equiv -\alpha \text{ (mod. } p^\pi);$$

also hat die Congruenz (1) entweder gar keine Wurzel, oder sie hat zwei incongruente Wurzeln α und $-\alpha$.

Es ist nun noch zu entscheiden, wann das Eine, wann das Andere Statt finden wird. Da nun jede Wurzel α der Congruenz (1) auch eine Wurzel der Congruenz

$$x^2 \equiv D \text{ (mod. } p) \tag{2}$$

ist, so leuchtet ein, dass die Congruenz (1) nur dann möglich ist, wenn D quadratischer Rest von p ist; es fragt sich daher nur, ob auch umgekehrt, wenn D quadratischer Rest von p ist, hieraus die Möglichkeit der Congruenz (1) folgt. Um dies zu zeigen, brauchen wir nur nachzuweisen, dass, sobald die Congruenz (2) eine Wurzel α besitzt (also D quadratischer Rest von p ist), hieraus sich eine Wurzel der Congruenz (1) ableiten lässt, welche $\equiv \alpha$ (mod. p) ist; und da Aehnliches von jeder Congruenz $x^2 \equiv D$ (mod. k) gilt, wo D stets dieselbe Zahl, k aber irgend eine Potenz der Primzahl p ist, so braucht man nur zu zeigen, dass aus einer Wurzel α der Congruenz (1) sich eine Wurzel der Congruenz

$$x^2 \equiv D \text{ (mod. } p^{\pi+1}) \tag{3}$$

ableiten lässt, welche $\equiv \alpha$ (mod. p^π) ist. Es sei daher

$$\alpha^2 \equiv D \text{ (mod. } p^\pi) \quad \text{oder} \quad \alpha^2 - D = hp^\pi,$$

so setzen wir

$$x = \alpha + p^\pi y,$$

woraus

$$x^2 - D = hp^\pi + 2\alpha p^\pi y + p^{2\pi} y^2 \equiv p^\pi (h + 2\alpha y) \text{ (mod. } p^{\pi+1})$$

folgt; damit nun $x^2 \equiv D$ (mod. $p^{\pi+1}$) werde, braucht y nur so bestimmt zu werden, dass

$$2\alpha y \equiv -h \text{ (mod. } p)$$

werde; da nun D, folglich auch α und also, da p ungerade ist, auch 2α eine durch p nicht theilbare Zahl ist, so lässt sich y stets so wählen, dass es dieser Congruenz ersten Grades genügt. Wir sehen also, dass aus der Möglichkeit der Congruenz (1) auch

stets die Möglichkeit der Congruenz (3) folgt; durch dieselbe wiederholt angewendete Schlussweise ergiebt sich also auch, dass aus der Möglichkeit der Congruenz (2) stets die der Congruenz (1) folgt, und wir haben auch eine Methode gefunden, um aus einer Wurzel der Congruenz $x^2 \equiv D$ für den Modul p successive eine Wurzel derselben Congruenz für die Moduln p^2, $p^3 \ldots p^n$ zu gewinnen. Wir haben mithin folgendes Resultat:

Ist p eine ungerade Primzahl, und D eine durch p nicht theilbare Zahl, so ist für die Möglichkeit der Congruenz

$$x^2 \equiv D \text{ (mod. } p^n)$$

erforderlich und hinreichend, dass

$$\left(\frac{D}{p}\right) = 1,$$

d. h. dass D quadratischer Rest von p sei; sobald diese Bedingung erfüllt ist, besitzt die vorgelegte Congruenz zwei incongruente Wurzeln α und $-\alpha$, welche gefunden werden können, sobald man eine Wurzel der Congruenz

$$x^2 \equiv D \text{ (mod. } p)$$

gefunden hat.

§. 36.

Wir gehen nun zu dem besondern Fall über, in welchem der Modul k eine Potenz der Primzahl 2 ist, so dass also D irgend eine ungerade Zahl bedeutet. Betrachten wir zunächst die Congruenz

$$x^2 \equiv D \text{ (mod. } 4),$$

so erkennt man leicht, dass dieselbe stets und nur dann möglich ist, wenn

$$D \equiv 1 \text{ (mod. } 4)$$

ist. Denn ist die Congruenz möglich, so ist x jedenfalls ungerade, und das Quadrat von $x = 2n + 1$ ist $4n^2 + 4n + 1 \equiv 1$ (mod. 4); umgekehrt, ist $D \equiv 1$ (mod. 4), so hat die Congruenz offenbar die beiden incongruenten Wurzeln $x \equiv 1$ und $x \equiv -1$ (mod. 4).

Gehen wir nun zu der Congruenz

$$x^2 \equiv D \text{ (mod. } 8)$$

über, so leuchtet ein, da das Quadrat einer jeden ungeraden Zahl $4n \pm 1$ gleich $16n^2 \pm 8n + 1 \equiv 1 \pmod{8}$ ist, dass diese Congruenz nur dann möglich ist, wenn

$$D \equiv 1 \pmod{8}$$

ist; und umgekehrt, sobald diese Bedingung erfüllt ist, hat die Congruenz die vier incongruenten Wurzeln $x \equiv 1$, $x \equiv 3$, $x \equiv 5$, $x \equiv 7$.

Betrachten wir jetzt die Congruenz

$$x^2 \equiv D \pmod{2^\pi},$$

wo $\pi \geqq 3$ ist, so kann diese Congruenz nur dann möglich sein, wenn die Congruenz

$$x^2 \equiv D \pmod{8}$$

möglich ist; es ist daher erforderlich, dass

$$D \equiv 1 \pmod{8}$$

sei. Wir wollen nun umgekehrt zeigen, dass diese Bedingung auch hinreicht, und dass dann die Congruenz stets 4 incongruente Wurzeln hat. Nehmen wir nämlich an, dies sei für den Modul 2^π schon bewiesen, so können wir zeigen, dass Dasselbe auch für den Modul $2^{\pi+1}$ gilt. Es sei nämlich α eine Wurzel der Congruenz

$$x^2 \equiv D \pmod{2^\pi}$$

also

$$\alpha^2 - D = h \cdot 2^\pi,$$

so setzen wir

$$x = \alpha + 2^{\pi-1} \cdot y;$$

dann wird

$$x^2 - D = h \cdot 2^\pi + 2^\pi \cdot \alpha y + 2^{2\pi-2} y^2.$$

Da nun $\pi \geqq 3$, so ist $2\pi - 2 \geqq \pi + 1$, folglich

$$x^2 - D \equiv 2^\pi (h + \alpha y) \pmod{2^{\pi+1}}.$$

Damit also $x^2 - D$ durch $2^{\pi+1}$ theilbar werde, braucht man nur y so zu wählen, dass

$$\alpha y \equiv -h \pmod{2}$$

werde. Dies ist aber stets möglich, da α eine ungerade Zahl ist; also folgt aus der Möglichkeit der Congruenz

$$x^2 \equiv D \pmod{2^\pi},$$

wo $\pi \geqq 3$ ist, stets die Möglichkeit der Congruenz

$$x^2 \equiv D \pmod{2^{\pi+1}}.$$

Wir schliessen hieraus zunächst das folgende Resultat:

Damit die Congruenz

$$x^2 \equiv D \pmod{2^\pi},$$

in welcher $\pi \geqq 3$ *ist, Wurzeln habe, ist erforderlich und hinreichend, dass*

$$D \equiv 1 \pmod{8}$$

sei.

Ist nun α eine Wurzel dieser Congruenz — und eine solche kann immer nach der obigen Methode gefunden werden —, so muss, wenn x irgend eine Wurzel derselben Congruenz bezeichnet,

$$x^2 - \alpha^2 = (x - \alpha)(x + \alpha) \equiv 0 \pmod{2^\pi}$$

sein. Da ferner α sowohl wie x ungerade Zahlen sein müssen, so sind die beiden Factoren $x - \alpha$ und $x + \alpha$ gerade Zahlen, und dann muss

$$\frac{x - \alpha}{2} \cdot \frac{x + \alpha}{2} \equiv 0 \pmod{2^{\pi - 2}}$$

sein. Da nun die Differenz der beiden Factoren $\frac{1}{2}(x - \alpha)$ und $\frac{1}{2}(x + \alpha)$ eine ungerade Zahl ist, so muss einer von ihnen ungerade, und der andere folglich theilbar durch $2^{\pi - 2}$ sein. Dies giebt folgende Fälle:

$$x \equiv \alpha \pmod{2^{\pi - 1}} \quad \text{oder} \quad x \equiv -\alpha \pmod{2^{\pi - 1}}$$

und diese liefern wieder folgende vier Fälle:

$$x \equiv \alpha \pmod{2^\pi}; \quad x \equiv \alpha + 2^{\pi - 1} \pmod{2^\pi};$$

$$x \equiv -\alpha \pmod{2^\pi}; \quad x \equiv -\alpha - 2^{\pi - 1} \pmod{2^\pi}.$$

Und umgekehrt überzeugt man sich leicht, dass jede dieser vier in Bezug auf den Modul 2^π incongruenten Zahlen der Congruenz genügt.

Wir fassen die ganze Untersuchung in folgendem Satze zusammen:

Die Congruenz

$$x^2 \equiv D \pmod{2^\pi}$$

ist 1) *stets möglich, wenn* $\pi = 1$, *und hat dann eine Wurzel;* 2) *sie ist, wenn* $\pi = 2$, *stets und nur dann möglich, wenn* $D \equiv 1$ (*mod.* 4), *und sie hat dann zwei Wurzeln;* 3) *sie ist, wenn* $\pi \geqq 3$, *stets und nur dann möglich, wenn* $D \equiv 1$ (*mod.* 8) *ist, und zwar hat sie dann vier Wurzeln.*

§. 37.

Es ist jetzt leicht, die Möglichkeit und die Anzahl der Wurzeln der Congruenz $x^2 \equiv D$ für einen beliebigen Modulus zu beurtheilen, der relative Primzahl zu D ist. Wir führen diese Untersuchung ganz allgemein in folgender Weise.

Es seien $a, b, c \ldots$ relative Primzahlen zu einander, und

$$f(x) \equiv 0 \pmod{a\,b\,c \ldots} \qquad (1)$$

eine beliebige zur Auflösung vorgelegte Congruenz, so lässt dieselbe sich stets auf die vollständige Auflösung der Congruenzen

$$\left.\begin{array}{l} f(x) \equiv 0 \pmod{a} \\ f(x) \equiv 0 \pmod{b} \\ f(x) \equiv 0 \pmod{c} \\ \text{u. s. w.} \end{array}\right\} \qquad (2)$$

zurückführen. Zunächst leuchtet ein, dass jede Wurzel x der Congruenz (1) auch allen Congruenzen (2) genügen muss; es wird daher die Congruenz (1) unmöglich sein, wenn dies mit irgend einer der Congruenzen (2) der Fall ist. Umgekehrt, ist α irgend eine Wurzel der Congruenz $f(x) \equiv 0$ (mod. a), ebenso β irgend eine Wurzel der Congruenz $f(x) \equiv 0$ (mod. b), γ eine Wurzel der Congruenz $f(x) \equiv 0$ (mod. c) u. s. w., so bestimme man (nach §. 25) eine Zahl x durch das System von Congruenzen

$$\left.\begin{array}{l} x \equiv \alpha \pmod{a} \\ x \equiv \beta \pmod{b} \\ x \equiv \gamma \pmod{c} \\ \text{u. s. w.,} \end{array}\right\} \qquad (3)$$

so wird

$$f(x) \equiv f(\alpha) \equiv 0 \pmod{a}$$
$$f(x) \equiv f(\beta) \equiv 0 \pmod{b}$$
$$f(x) \equiv f(\gamma) \equiv 0 \pmod{c}$$
u. s. w.

und folglich, da $a, b, c \ldots$ relative Primzahlen zu einander sind, auch

$$f(x) \equiv 0 \pmod{abc \ldots},$$

d. h. jede dem System (3) genügende Zahl x ist eine Wurzel der vorgelegten Congruenz (1). Da nun (nach §. 25) dem System (3) unendlich viele Zahlen x genügen, welche aber alle nach dem Modul $abc \ldots$ einander congruent sind, so liefert das System (3) eine und nur eine Wurzel x der Congruenz (1). Ist nun

λ die Anzahl aller incongruenten Wurzeln α (mod. a)
μ " " " " " β (mod. b)
ν " " " " " γ (mod. c)
u. s. w.,

so kann man im Ganzen $\lambda\mu\nu \ldots$ verschiedene Systeme (3) bilden, welchen (nach §. 25) ebensoviele verschiedene Wurzeln x der Congruenz (1) entsprechen; und andere Wurzeln kann diese letztere nicht besitzen, weil, wie schon oben bemerkt ist, jede bestimmte Wurzel x der Congruenz (1) auch Wurzel aller Congruenzen (2) und folglich einem bestimmten α (mod. a), einem bestimmten β (mod. b), einem bestimmten γ (mod. c) u. s. f. congruent sein muss. Mithin ist die Anzahl aller nach dem Modul $abc \ldots$ incongruenten Wurzeln der vorgelegten Congruenz $= \lambda\mu\nu \ldots$

Mit Hülfe dieses allgemeinen Resultates sind wir im Stande zu beurtheilen, ob die Congruenz

$$x^2 \equiv D \pmod{k},$$

in welcher D und k relative Primzahlen sind, möglich, und wie gross die Anzahl σ ihrer incongruenten Wurzeln ist. Bedeutet p jede beliebige in dem Modul k (also nicht in D) aufgehende ungerade Primzahl, so ist erforderlich, dass

$$\left(\frac{D}{p}\right) = +1$$

sei; ist diese Bedingung erfüllt, so hat die Congruenz $x^2 \equiv D$ in Bezug auf jeden Modulus von der Form p^π genau zwei incongruente Wurzeln. Ist daher der Modul k ungerade, und μ die Anzahl der von einander verschiedenen in k aufgehenden Primzahlen p, so ist

$$\sigma = 2^\mu.$$

Dasselbe ist der Fall, wenn der Modulus k das Doppelte einer ungeraden Zahl ist; denn die Congruenz $x^2 \equiv D$ (mod. 2) hat stets eine und nur eine Wurzel.

Ist aber k das Vierfache einer ungeraden Zahl, so ist ausser den früheren μ Bedingungen $\left(\frac{D}{p}\right) = +1$ noch erforderlich, dass $D \equiv 1$ (mod. 4) sei; da alsdann die Congruenz $x^2 \equiv D$ (mod. 4) zwei Wurzeln besitzt, so ist

$$\sigma = 2^{\mu+1}.$$

Ist endlich $k \equiv 0$ (mod. 8), so ist ausser den früheren μ Bedingungen $\left(\frac{D}{p}\right) = +1$ noch erforderlich, dass $D \equiv 1$ (mod. 8) sei; da dann die Congruenz $x^2 \equiv D$ (mod. 2^π), wo $\pi \geqq 3$, stets vier Wurzeln hat, so ist in diesem Fall

$$\sigma = 2^{\mu+2}.$$

§. 38.

Bevor wir diesen Gegenstand verlassen, wollen wir noch eine Anwendung von dem soeben gewonnenen Resultate auf eine Verallgemeinerung des Wilson'schen Satzes (§. 27) machen. Setzen wir $D = 1$, so ergiebt sich, dass die Congruenz

$$x^2 \equiv 1 \pmod{k} \qquad (1)$$

für jeden Modul k möglich ist; die Anzahl σ ihrer Wurzeln ist $= 1$, wenn $k = 1$ oder $k = 2$; sie ist $= 2$, wenn k eine Potenz einer ungeraden Primzahl oder das Doppelte einer solchen Potenz oder $= 4$ ist; in allen übrigen Fällen ist σ durch 4 theilbar. Schliessen wir die Fälle $k = 1$ und $k = 2$ aus, so zerfallen die

σ Wurzeln in $\frac{1}{2}\sigma$ Paare von Wurzeln ϱ und $-\varrho$; denn mit ϱ ist gleichzeitig auch $-\varrho$ eine Wurzel, und da ϱ relative Primzahl zu k, und folglich 2ϱ nicht $\equiv 0 \pmod{k}$ sein kann, so sind je zwei solche Wurzeln ϱ und $-\varrho$ auch incongruent. Das Product $\varrho \times (-\varrho) = -\varrho^2$ zweier solcher Wurzeln ist $\equiv -1$, und folglich ist das Product aller σ Wurzeln $\equiv +1$ oder -1, je nachdem σ durch 4 theilbar ist oder nicht.

Unter den $\varphi(k)$ Zahlen z, welche nicht grösser als k und relative Primzahlen zu k sind, finden sich zunächst die σ Wurzeln der Congruenz (1); die übrigen $\varphi(k) - \sigma$ dieser Zahlen z (wenn noch solche vorhanden sind) lassen sich in Paare von je zwei solchen Zahlen r und s zerlegen, deren Product $rs \equiv 1$ ist; denn zu jeder Zahl r gehört (nach §. 22) eine solche Zahl s und nur eine, und ausserdem kann s nicht $\equiv r$ sein, weil sonst $r^2 \equiv 1$, und folglich r eine der σ Wurzeln der Congruenz (1) wäre. Mithin ist auch das Product aller dieser $\varphi(k) - \sigma$ Zahlen $\equiv 1$.

Multiplicirt man daher alle $\varphi(k)$ Zahlen z mit einander, so wird das Product $\equiv -1$, wenn k Potenz einer ungeraden Primzahl oder das Doppelte einer solchen Potenz oder $= 4$ ist, in allen übrigen Fällen aber $\equiv +1$. (In den beiden ausgeschlossenen Fällen $k = 1$ und $k = 2$ ist $\varphi(k) = 1$, und die einzige Zahl $z \equiv \pm 1$.) Dies ist der verallgemeinerte Wilson'sche Satz.

§. 39.

Nachdem in den vorhergehenden Paragraphen die erste der beiden in §. 32 aufgeworfenen Fragen ihre vollständige Beantwortung gefunden hat, wenden wir uns jetzt zu der zweiten ungleich interessanteren, aber auch schwierigern Aufgabe:

Alle Moduln k zu finden, von welchen eine gegebene Zahl D quadratischer Rest ist.

Bevor wir zu der Lösung derselben übergehen, wollen wir erwähnen, dass man häufig, namentlich in den älteren Schriften, eine andere Ausdrucksweise vorfindet. Die Moduln k, für welche eine Congruenz $f(x) \equiv 0 \pmod{k}$ möglich ist, nennt man auch *Divisoren der Form* $f(x)$, weil es Zahlen x giebt, für welche $f(x)$ durch einen solchen Modul k theilbar wird; die von uns gesuchten Zahlen k sind daher die Divisoren der Form $x^2 - D$; sie stimmen vollständig überein mit den Divisoren der Form $t^2 - Du^2$,

in welcher t, u zwei unbestimmte ganze Zahlen bedeuten, die aber immer relative Primzahlen zu einander sein müssen. Dass wirklich jeder Divisor der Form $x^2 - D$ auch ein Divisor der Form $t^2 - Du^2$ ist, leuchtet unmittelbar ein, da die letztere in die erstere übergeht, wenn man $t = x$, $u = 1$ setzt. Umgekehrt, ist k Divisor der Form $t^2 - Du^2$, so ist u jedenfalls relative Primzahl zu k (denn ginge irgend eine Primzahl gleichzeitig in k und u auf, so müsste sie auch in t^2 und folglich auch in t aufgehen, gegen die Voraussetzung, dass t, u relative Primzahlen sind), und man kann folglich eine Zahl x finden, welche der Congruenz $ux \equiv t \pmod{k}$ genügt; da nun $t^2 - Du^2 \equiv 0 \pmod{k}$, so ist auch $u^2(x^2 - D) \equiv 0 \pmod{k}$ und folglich, da u^2 relative Primzahl zu k ist, auch $x^2 - D \equiv 0 \pmod{k}$, d. h. jeder Divisor k der Form $t^2 - Du^2$, in welcher t und u relative Primzahlen zu einander sind, ist auch Divisor der Form $x^2 - D$.

Das allgemeine Problem wird daher häufig auch so ausgedrückt: es sollen alle Divisoren der Form $t^2 - Du^2$ gefunden werden, in welcher D eine gegebene, t und u dagegen zwei unbestimmte ganze Zahlen bedeuten, die relative Primzahlen zu einander sind.

Wir beschränken uns auch hier auf solche (immer mit *positivem* Vorzeichen genommene) Moduln k, die relative Primzahlen zu D sind; da ferner nach den vorhergehenden Untersuchungen die Möglichkeit der Congruenz $x^2 \equiv D \pmod{k}$ nur von der Beschaffenheit der in k aufgehenden Primzahlen abhängt und für einen Modul von der Form 2^π immer leicht beurtheilt werden kann, so kommt es nur darauf an, alle ungeraden (in D nicht aufgehenden) Primzahlen p zu finden, von welchen D quadratischer Rest ist. Bedenken wir ferner, dass (nach §. 33) der quadratische Charakter einer Zahl D in Bezug auf einen solchen Modulus p nur von den in D enthaltenen Factoren abhängt, so werden wir in letzter Instanz auf folgendes Problem geführt:

Alle ungeraden Primzahlen p zu finden, für welche irgend eine der drei Congruenzen

$$x^2 \equiv -1, \quad x^2 \equiv 2, \quad x^2 \equiv q \pmod{p}$$

möglich ist, wo q irgend eine gegebene positive ungerade Primzahl bedeutet.

§. 40.

Die Auffindung aller ungeraden Primzahlen p, für welche die Congruenz

$$x^2 \equiv -1 \pmod{p}$$

möglich ist, bietet keine Schwierigkeit mehr dar. Denn da (nach §. 33) allgemein

$$\left(\frac{D}{p}\right) \equiv D^{\frac{p-1}{2}} \pmod{p}$$

ist, so erhält man speciell

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$$

und folglich auch

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

In Worten lautet dieser wichtige Satz folgendermaassen:

Die Zahl -1 *ist quadratischer Rest aller Primzahlen von der Form* $4n + 1$, *dagegen quadratischer Nichtrest aller Primzahlen von der Form* $4n + 3$.

Dasselbe Resultat erhält man auch auf folgendem Wege. Ist die Congruenz $x^2 \equiv -1 \pmod{p}$ möglich, und x eine Wurzel derselben, so folgt hieraus durch Potenzirung

$$x^{p-1} \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$$

und hieraus (nach dem Fermat'schen Satze §. 19) $(-1)^{\frac{p-1}{2}} = 1$ also $p = 4n + 1$; d. h. die Zahl -1 ist quadratischer Nichtrest von allen Primzahlen von der Form $4n + 3$. Ist umgekehrt p von der Form $4n + 1$, so ist $x^{p-1} - 1$ algebraisch theilbar durch $x^4 - 1$, also auch durch $x^2 + 1$; es ist folglich

$$x^{p-1} - 1 = (x^2 + 1)\,\psi(x),$$

wo $\psi(x)$ ein Polynom mit ganzen Coefficienten bedeutet; da nun (nach dem Fermat'schen Satze §. 19) die linke Seite dieser Gleichung für $p-1$ incongruente Werthe von x congruent Null wird, so wird (nach §. 26) auch $x^2 + 1$ für zwei incongruente Werthe

von x congruent Null*), d. h. die Zahl -1 ist quadratischer Rest von allen Primzahlen von der Form $4n + 1$. Der Satz ist also von Neuem bewiesen.

§. 41.

Wir gehen nun zu der Lösung der zweiten Aufgabe über, welche sich auf die Congruenz

$$x^2 \equiv 2 \pmod{p}$$

bezieht. *Fermat* hat, wahrscheinlich durch Induction, folgendes, zuerst von *Lagrange* bewiesenes, Resultat gefunden:

Die Zahl 2 *ist quadratischer Rest aller Primzahlen von einer der beiden Formen* $8n + 1$ *oder* $8n + 7$, *dagegen Nichtrest aller Primzahlen von einer der beiden Formen* $8n + 3$ *oder* $8n + 5$.

Wir beweisen zuerst den zweiten Theil des Satzes, dass nämlich 2 Nichtrest aller Primzahlen p von der Form $8n \pm 3$ ist. Offenbar ist derselbe für $p = 3$ richtig, denn nur die Zahl 1 ist Rest von 3. Gesetzt nun, der Satz wäre nicht allgemein gültig, so müsste es doch eine *kleinste* Primzahl p von der Form $8n \pm 3$ geben, für welche er unrichtig würde, für welche also die Congruenz

$$x^2 \equiv 2 \pmod{p}$$

möglich würde. Hierin kann man immer die Wurzel x kleiner als p und ungerade voraussetzen, denn wenn x gerade ist, so ist die andere Wurzel $x' = p - x$ ungerade. Wir können daher

$$x^2 - 2 = pf$$

setzen, wo f positiv und kleiner als p ist; da ferner x^2 von der Form $8n + 1$, also pf von der Form $8n - 1$, und folglich f von der Form $8n \mp 3$ ist, so hat die Zahl f mindestens einen Primfactor p' von einer der Formen $8n + 3$ oder $8n - 3$; denn ein Product aus lauter Factoren von der Form $8n \pm 1$ würde wieder

*) Man findet auch leicht mit Hülfe des Wilson'schen Satzes (§. 27), dass diese Wurzeln $\equiv \pm 1 \cdot 2 \cdot 3 \ldots \frac{1}{2}(p-1)$ sind.

dieselbe Form $8n \pm 1$ haben. Für diese Primzahl p', die jedenfalls $< p$ ist, würde dann ebenfalls $x^2 \equiv 2 \pmod{p'}$ sein; allein dies streitet mit unserer Voraussetzung, dass p die kleinste in der Form $8n \pm 3$ enthaltene Primzahl ist, von welcher die Zahl 2 quadratischer Rest ist. Mithin ist diese Voraussetzung überhaupt unzulässig, und es folgt, dass stets

$$\left(\frac{2}{p}\right) = -1 \text{ ist, wenn } p = 8n \pm 3.$$

Wir wollen jetzt zweitens beweisen, dass die Zahl 2 quadratischer Rest aller Primzahlen p von der Form $8n + 7$ ist; da nun (nach §. 40) -1 quadratischer Nichtrest aller dieser Primzahlen ist, so haben wir nur zu zeigen, dass die Zahl -2 ebenfalls Nichtrest aller dieser Primzahlen ist; statt dessen stellen wir uns die allgemeinere Aufgabe zu beweisen, dass -2 Nichtrest von allen in den beiden Formen $8n + 5$, $8n + 7$ enthaltenen Primzahlen ist, obgleich dies für die Primzahlen der Form $8n + 5$ von welchen (nach §. 40) -1 quadratischer Rest ist, schon im Vorhergehenden geschehen ist. Zunächst bemerken wir wieder, dass der Satz für die kleinste in einer dieser Formen enthaltene Primzahl 5 in der That richtig ist. Wenn nun der Satz nicht allgemein gültig ist, so sei p die kleinste ihm nicht gehorchende Primzahl, so dass also eine Zahl x existirt, für welche

$$x^2 + 2 \equiv 0 \pmod{p}$$

ist; auch hier können wir wieder annehmen, dass x kleiner als p und ungerade ist, so dass, wenn wir

$$x^2 + 2 = pf$$

setzen, die Zahl f positiv, ungerade und kleiner als p ausfällt. Da ferner $x^2 + 2 \equiv 3 \pmod{8}$ und $p \equiv 5$ oder $\equiv 7 \pmod{8}$ ist, so muss f entsprechend $\equiv 7$ oder $\equiv 5 \pmod{8}$ sein; und da ein Product aus lauter Factoren von den Formen $8n + 1$, oder $8n + 3$ stets wieder eine dieser Formen, niemals eine der Formen $8n + 5$ oder $8n + 7$ hat, so muss die Zahl f mindestens einen Primfactor p' von einer der Formen $8n + 7$, $8n + 5$ haben, für welchen der Satz ebenfalls unrichtig ist, da $x^2 + 2 \equiv 0 \pmod{p'}$ ist; allein, da $p' < p$, so streitet dies mit der Annahme, dass p die kleinste dem Satze nicht gehorchende Primzahl ist. Also ist die Annahme überhaupt nicht zulässig und folglich der Satz allgemeingültig, dass

$$\left(\frac{-2}{p}\right) = -1 \text{ für } p = 8n + 5 \text{ oder } = 8n + 7,$$

d. h. dass

$$\left(\frac{2}{p}\right) = -1 \text{ für } p = 8n + 5$$
$$\left(\frac{2}{p}\right) = +1 \text{ für } p = 8n + 7$$

ist.

Es bleibt jetzt nur noch zu beweisen übrig, dass 2 quadratischer Rest von allen Primzahlen p von der Form $8n + 1$ ist; hierauf ist die vorhergehende Methode aus dem Grunde nicht anwendbar, weil die Annahme des Gegentheils sich nicht in Form einer Congruenz darstellen lässt, die dann zur Auffindung des Widerspruchs benutzt werden könnte. Allein in diesem Falle kann man direct, wie folgt, verfahren; da $p = 8n + 1$ ist, so hat die Function $x^{p-1} - 1$ den Divisor $x^8 - 1$, also auch den Factor $x^4 + 1$, und hieraus folgt nach einem frühern Satze (§. 26), dass die Congruenz

$$x^4 + 1 \equiv 0 \pmod{p}$$

Wurzeln hat; ist nun x eine solche, so ist

$$x^4 + 1 = (x^2 \pm 1)^2 \mp 2x^2 \equiv 0 \pmod{p},$$

also

$$(x^2 \pm 1)^2 \equiv \pm 2x^2 \pmod{p};$$

es ist daher $\pm 2x^2$ und folglich auch ± 2 quadratischer Rest von p; in Zeichen

$$\left(\frac{\pm 2}{p}\right) = 1, \text{ wenn } p = 8n + 1.$$

Hiermit ist der Satz in allen seinen Theilen bewiesen; wir können denselben in der einen Gleichung

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

zusammenfassen; denn je nachdem $p = 8n \pm 1$, oder $p = 8n \pm 3$ ist, wird $\frac{1}{8}(p^2 - 1)$ eine gerade oder ungerade Zahl.

§. 42.

Wir kommen nun zu der Untersuchung der dritten Frage: *von welchen ungeraden Primzahlen p ist die gegebene ungerade Primzahl q quadratischer Rest?* Die vollständige Antwort hierauf wird durch einen der wichtigsten und interessantesten Sätze der Zahlentheorie gegeben, welcher seines eigenthümlichen Charakters wegen den Namen des *Reciprocitäts-Satzes* erhalten hat. Man kann ihn folgendermaassen aussprechen:

Sind p und q zwei positive ungerade Primzahlen, von denen mindestens eine die Form $4n + 1$ hat, so ist q quadratischer Rest oder Nichtrest von p, je nachdem p quadratischer Rest oder Nichtrest von q ist; haben aber beide Primzahlen p und q die Form $4n + 3$, so ist q quadratischer Rest oder Nichtrest von p, je nachdem p quadratischer Nichtrest oder quadratischer Rest von q ist.

Offenbar lässt sich dieser Satz in die für beide Fälle gültige Gleichung

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

zusammenfassen; denn sobald mindestens eine der beiden Primzahlen p oder q die Form $4n + 1$ hat, so ist die entsprechende der beiden Zahlen $\frac{1}{2}(p-1)$ oder $\frac{1}{2}(q-1)$, und folglich auch ihr Product $\frac{1}{2}(p-1) \cdot \frac{1}{2}(q-1)$ eine gerade Zahl, so dass

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = 1, \text{ d. h. } \left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$$

ist, worin der erste Fall seinen Ausdruck findet; sind dagegen beide Primzahlen p und q von der Form $4n + 3$, so sind auch beide Zahlen $\frac{1}{2}(p-1)$ und $\frac{1}{2}(q-1)$, und folglich auch ihr Product $\frac{1}{2}(p-1) \cdot \frac{1}{2}(q-1)$ ungerade, so dass

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = -1, \text{ d. h. } \left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right)$$

wird, worin der zweite Theil des Satzes ausgedrückt ist.

Ist z. B. $p = 3$, $q = 5$, so ist p quadratischer Nichtrest von q und gleichzeitig q quadratischer Nichtrest von p, in Zeichen

$$\left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = -1.$$

Ist ferner $p = 3$, $q = 13$, so ist p quadratischer Rest von q und gleichzeitig q quadratischer Rest von p, in Zeichen

$$\left(\frac{3}{13}\right) = \left(\frac{13}{3}\right) = +1.$$

Ist dagegen $p = 3$, $q = 7$, so ist p quadratischer Nichtrest von q und gleichzeitig q quadratischer Rest von p, in Zeichen

$$\left(\frac{3}{7}\right) = -\left(\frac{7}{3}\right) = -1.$$

Dieser Satz wurde zuerst von *Legendre* durch Induction gefunden und ausgesprochen; allein erst *Gauss* hat denselben vollständig bewiesen, ja er hat nach einander sechs auf ganz verschiedenen Grundgedanken beruhende Beweise von diesem Satze gegeben, den er in etwas anderer Form aussprach und seiner Wichtigkeit wegen das *Theorema fundamentale* in der Theorie der quadratischen Reste nannte. Wir folgen hier zunächst dem dritten dieser sechs Beweise, der sich auf ein Lemma stützt, durch welches das Euler'sche Kriterium (§. 33) über den Charakter einer Zahl D in Bezug auf die Primzahl p in ein anderes umgeformt wird.

§. 43.

Wir haben früher (§. 33) gesehen, dass eine durch p nicht theilbare Zahl D quadratischer Rest oder Nichtrest von p ist, je nachdem $D^{\frac{p-1}{2}} \equiv +1$ oder $\equiv -1 \pmod{p}$ ist; betrachten wir nun die Producte

$$D,\ 2D,\ 3D\ \ldots\ \frac{p-1}{2}D$$

aus dieser Zahl D und aus den ersten $\frac{1}{2}(p-1)$ ganzen positiven Zahlen, so werden die kleinsten positiven Reste

$$r_1,\ r_2,\ r_3\ \ldots\ r_{\frac{p-1}{2}}$$

derselben, nach dem Modulus p genommen, erstens sämmtlich verschieden von einander und kleiner als p sein, und keiner von ihnen kann gleich Null sein. Wir theilen nun diese $\frac{1}{2}(p-1)$ Reste in zwei Abtheilungen, je nachdem sie grösser oder kleiner als $\frac{1}{2}p$ sind, und bezeichnen die erstern, deren Anzahl $= \mu$ sei, mit

$$\alpha_1, \ \alpha_2 \ \ldots \ \alpha_\mu,$$

die übrigen $\frac{1}{2}(p-1) - \mu = \lambda$ Reste, welche kleiner als $\frac{1}{2}p$ sind, mit

$$\beta_1, \ \beta_2 \ \ldots \ \beta_\lambda.$$

Nimmt man nun von den erstern μ Resten ihre Ergänzungen zur Zahl p, also die Zahlen

$$p - \alpha_1, \ p - \alpha_2 \ \ldots \ p - \alpha_\mu,$$

so liegen dieselben, ebenso wie die λ Zahlen $\beta_1, \beta_2 \ldots \beta_\lambda$, auch zwischen den Grenzen 0 und $\frac{1}{2}p$; ausserdem sind sie alle von einander verschieden; endlich lässt sich aber auch zeigen, dass sie von den λ Zahlen $\beta_1, \beta_2 \ldots \beta_\lambda$ verschieden sind; denn wäre z. B. $p - \alpha = \beta$, also $\alpha + \beta = p \equiv 0$ (mod. p), so müsste auch, wenn α der Rest von sD, β der Rest von tD ist,

$$sD + tD = (s+t)D \equiv 0 \text{ (mod. } p)$$

und folglich $s + t$ durch p theilbar sein; allein da jede der beiden Zahlen s und t zwischen 0 und $\frac{1}{2}p$ liegt, so liegt $s + t$ zwischen 0 und p (mit Ausschluss dieser beiden Grenzen); es kann daher $s + t$ nicht theilbar durch p, und folglich auch nicht $p - \alpha = \beta$ sein.

Mithin haben die folgenden $\lambda + \mu = \frac{1}{2}(p-1)$ Zahlen

$$p - \alpha_1, \ p - \alpha_2 \ \ldots \ p - \alpha_\mu; \ \beta_1, \ \beta_2 \ \ldots \ \beta_\lambda$$

lauter von einander verschiedene Werthe, und da sie ihrem Werth nach zwischen 0 und $\frac{1}{2}p$ liegen, so müssen sie im Complex genommen identisch mit den $\frac{1}{2}(p-1)$ Zahlen

$$1, \ 2, \ 3 \ \ldots \ \frac{p-1}{2}$$

sein, so dass ihr Product

$$(p-\alpha_1)(p-\alpha_2)\cdots(p-\alpha_\mu)\,\beta_1\beta_2\cdots\beta_\lambda = 1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2}$$

ist. Werfen wir hieraus die Multipla von p weg, so erhalten wir die Congruenz

$$(-1)^\mu\,\alpha_1\alpha_2\cdots\alpha_\mu\cdot\beta_1\beta_2\cdots\beta_\lambda \equiv 1\cdot2\cdot3\cdots\frac{p-1}{2} \text{ (mod. } p);$$

da nun andererseits

$$\alpha_1\, \alpha_2 \cdots \alpha_\mu \cdot \beta_1\, \beta_2 \cdots \beta_\lambda \equiv 1 \cdot 2 \cdots \frac{p-1}{2} D^{\frac{p-1}{2}} \pmod{p}$$

ist, so folgt hieraus, dass

$$(-1)^\mu \cdot 1 \cdot 2 \cdots \frac{p-1}{2} \cdot D^{\frac{p-1}{2}} \equiv 1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2} \pmod{p}$$

und also auch

$$D^{\frac{p-1}{2}} \equiv (-1)^\mu \pmod{p}$$

oder, was dasselbe sagt, dass

$$\left(\frac{D}{p}\right) = (-1)^\mu$$

ist. Hierin besteht die Umformung des Kennzeichens, welches darüber entscheidet, ob eine Zahl D quadratischer Rest oder Nichtrest der ungeraden Primzahl p ist:

Man braucht nur nachzusehen, ob die Anzahl μ der kleinsten positiven Reste der Zahlen

$$D,\ 2D,\ 3D\ \ldots\ \frac{p-1}{2} D,$$

die grösser als $\frac{1}{2}p$ ausfallen, gerade oder ungerade ist; je nachdem das Erstere oder Letztere eintritt, ist D quadratischer Rest oder quadratischer Nichtrest von p.

Mit Hülfe dieses Satzes ist man schon im Stande, für jedes wirklich gegebene D die Formen für die Primzahlen aufzustellen, von welchen D Rest oder Nichtrest ist. Um dies deutlicher zu zeigen, betrachten wir den allerdings schon früher (§. 41) vollständig durchgeführten Fall $D = 2$. Bilden wir die Zahlen

$$2,\ 4,\ 6\ \ldots\ (p-1),$$

so ist jede derselben auch ihr eigener kleinster positiver Rest in Bezug auf den Modulus p; es fragt sich daher nur, wieviele dieser Zahlen grösser als $\frac{1}{2}p$ sind. Es sei nun $2s$ die letzte dieser Zahlen, welche $< \frac{1}{2}p$ ist, so dass $2(s+1) > \frac{1}{2}p$ ist; dann ist

$$s < \frac{1}{4}p, \quad s+1 > \frac{1}{4}p,$$

d. h. s ist die grösste ganze in dem Bruch $\frac{1}{4}p$ enthaltene ganze Zahl, die wir im Folgenden durch das Symbol $[\frac{1}{4}p]$ bezeichnen

wollen. Hieraus folgt, dass die Anzahl μ derjenigen der obigen $\frac{1}{2}(p-1)$ Zahlen, welche $> \frac{1}{2}p$ sind, gleich

$$\frac{p-1}{2} - \left[\frac{p}{4}\right]$$

ist. Um nun zu entscheiden, ob diese Anzahl μ gerade oder ungerade ist, betrachten wir die folgenden vier Fälle:

1) Ist $p = 8n + 1$, so ist $\frac{p}{4} = 2n + \frac{1}{4}$, also $\left[\frac{p}{4}\right] = 2n$ und $\mu = \frac{p-1}{2} - \left[\frac{p}{4}\right] = 4n - 2n = 2n$;

folglich ist in diesem Fall

$$\left(\frac{2}{p}\right) = +1.$$

2) Ist $p = 8n + 3$, so ist $\frac{p}{4} = 2n + \frac{3}{4}$, also $\left[\frac{p}{4}\right] = 2n$ und $\mu = \frac{p-1}{2} - \left[\frac{p}{4}\right] = 4n + 1 - 2n = 2n + 1$;

folglich ist in diesem Fall

$$\left(\frac{2}{p}\right) = -1.$$

3) Ist $p = 8n + 5$, so ist $\frac{p}{4} = 2n + 1 + \frac{1}{4}$, also $\left[\frac{p}{4}\right] = 2n + 1$ und

$$\mu = \frac{p-1}{2} - \left[\frac{p}{4}\right] = 4n + 2 - (2n + 1) = 2n + 1;$$

folglich ist in diesem Fall

$$\left(\frac{2}{p}\right) = -1.$$

4) Ist endlich $p = 8n + 7$, so ist $\frac{p}{4} = 2n + 1 + \frac{3}{4}$, also $\left[\frac{p}{4}\right] = 2n + 1$ und

$$\mu = \frac{p-1}{2} - \left[\frac{p}{4}\right] = 4n + 3 - (2n + 1) = 2n + 2;$$

folglich ist in diesem Fall

$$\left(\frac{2}{p}\right) = +1.$$

Auf diese Weise finden wir also eine vollständige Bestätigung des Resultats unserer frühern Untersuchung (§. 41), und ganz ebenso würde sich für jeden speciellen Werth von D die Untersuchung führen lassen, z. B. für die nächstliegenden Fälle $D = 3$, $D = 5$ u. s. w.

§. 44.

Wir verlassen diese Anwendungen auf specielle Fälle und wenden uns zu einer weitern Umformung, bei welcher wir der spätern Bezeichnung wegen q statt D schreiben wollen. Bezeichnen wir allgemein mit $[x]$ die grösste in dem Werth x enthaltene ganze Zahl, so dass

$$0 \leqq x - [x] < 1$$

ist, so können wir

$$q = p\left[\frac{q}{p}\right] + r_1, \quad 2q = p\left[\frac{2q}{p}\right] + r_2 \ldots$$

$$\frac{p-1}{2} q = p\left[\frac{\frac{1}{2}(p-1)q}{p}\right] + r_{\frac{p-1}{2}}$$

setzen, worin wie früher (§. 43)

$$r_1, \; r_2 \; \ldots \; r_{\frac{p-1}{2}}$$

zwischen den Grenzen 0 und p liegen; theilen wir wieder diese kleinsten Reste in zwei Abtheilungen

$$\alpha_1, \; \alpha_2 \; \ldots \; \alpha_\mu$$

und

$$\beta_1, \; \beta_2 \; \ldots \; \beta_\lambda.$$

von denen die erstern $> \frac{1}{2} p$, die letztern $< \frac{1}{2} p$ sind, und bezeichnen wir mit A die Summe der μ erstern, mit B die Summe der λ letztern, ferner mit M die Summe

$$M = \left[\frac{q}{p}\right] + \left[\frac{2q}{p}\right] + \cdots + \left[\frac{\frac{1}{2}(p-1)q}{p}\right],$$

so folgt durch Addition der vorstehenden Gleichungen

$$\frac{p^2-1}{8} q = pM + A + B;$$

da nun (nach §. 43) der Complex der Zahlen

$$p-\alpha_1, \; p-\alpha_2 \ldots p-\alpha_\mu; \;\; \beta_1, \beta_2 \ldots \beta_\lambda$$

mit dem Complex der Zahlen

$$1, 2, 3 \ldots \frac{p-1}{2}$$

vollständig übereinstimmt, so ist ihre Summe

$$\frac{p^2-1}{8} = \mu p - A + B;$$

zieht man diese Gleichung von der vorhergehenden ab, so erhält man

$$\frac{p^2-1}{8}(q-1) = (M-\mu)p + 2A.$$

Nun kommt es uns lediglich darauf an, zu erfahren, ob μ gerade oder ungerade ist; lassen wir daher alle Multipla von 2 fort, so erhalten wir, da $p \equiv -1 \pmod{2}$ gesetzt werden kann,

$$\mu \equiv M + \frac{p^2-1}{8}(q-1) \pmod{2}.$$

Je nachdem daher die zur Rechten befindliche Zahl gerade oder ungerade ist, wird q quadratischer Rest oder Nichtrest von p sein. Nehmen wir daher z. B. wieder den Fall $q = 2$, so ergiebt sich unmittelbar $M = 0$, also

$$\mu \equiv \frac{p^2-1}{8} \pmod{2},$$

folglich

$$\left(\frac{2}{p}\right) = (-1)^\mu = (-1)^{\frac{p^2-1}{8}};$$

dies ist aber genau die schon früher (§. 41) aufgestellte Formel.

Von jetzt an wollen wir die Untersuchung nur noch unter der Voraussetzung fortführen, dass q eine positive ungerade, also $q-1$ eine gerade Zahl ist; dann ist also

$$\mu \equiv M \ (\text{mod. } 2), \ \left(\frac{q}{p}\right) = (-1)^M;$$

und es reducirt sich daher die ganze Frage darauf, zu entscheiden, ob die oben mit M bezeichnete Summe gerade oder ungerade ist.

Nehmen wir an, es sei $q < p$, so ist in der Reihe

$$\left[\frac{q}{p}\right], \ \left[\frac{2q}{p}\right] \ . \ . \ . \ \left[\frac{\frac{1}{2}(p-1)q}{p}\right]$$

jedes Glied höchstens um eine Einheit grösser als das unmittelbar vorhergehende; denn da

$$\frac{(s+1)q}{p} = \frac{sq}{p} + \frac{q}{p}$$

und

$$\frac{sq}{p} = \left[\frac{sq}{p}\right] + \delta$$

ist, wo δ einen echten Bruch bezeichnet, so ist

$$\frac{(s+1)q}{p} = \left[\frac{sq}{p}\right] + \delta + \frac{q}{p},$$

folglich, da die Summe der beiden echten Brüche δ und $\frac{q}{p}$ nothwendig kleiner als 2 ist,

$$\left[\frac{(s+1)q}{p}\right] = \left[\frac{sq}{p}\right] \ \text{oder} = \left[\frac{sq}{p}\right] + 1.$$

Da ferner

$$\frac{\frac{1}{2}(p-1)q}{p} = \frac{q-1}{2} + \frac{p-q}{2p}$$

ist, so ist der Werth des letzten Gliedes in der obigen Reihe

$$\left[\frac{\frac{1}{2}(p-1)q}{p}\right] = \frac{q-1}{2}.$$

Wenn nun s die ganzen Zahlen 1, 2 . . . bis $\frac{1}{2}(p-1)$ durchläuft, so haben wir vorzüglich auf die Werthe von s zu achten, von welchen ab der Werth des Symbols $\left[\frac{sq}{p}\right]$ um eine Einheit zunimmt, in der Weise, dass

$$\left[\frac{sq}{p}\right] = t - 1, \left[\frac{(s+1)q}{p}\right] = t$$

ist, wo t irgend eine der Zahlen

$$1, 2 \ldots \frac{q-1}{2}$$

bedeutet. Aus diesen beiden Gleichungen folgt aber

$$\frac{sq}{p} < t; \quad \frac{(s+1)q}{p} > t$$

(der Fall $(s+1)q = tp$ kann nicht eintreten, da weder q noch $(s+1)$ durch p theilbar ist) oder, was dasselbe ist,

$$s < \frac{tp}{q} < s + 1,$$

also

$$s = \left[\frac{tp}{q}\right].$$

In der Reihe M giebt es daher

$$\left[\frac{p}{q}\right] \quad \text{Glieder, welche den Werth } t - 1 = 0$$

$$\left[\frac{2p}{q}\right] - \left[\frac{p}{q}\right] \quad \text{,, ,, ,, ,,} \quad t - 1 = 1$$

. . . .

$$\left[\frac{tp}{q}\right] - \left[\frac{(t-1)p}{q}\right] \quad \text{,, ,, ,, ,,} \quad t - 1$$

. . . .

$$\frac{p-1}{2} - \left[\frac{\frac{1}{2}(q-1)p}{q}\right] \quad \text{,, ,, ,, ,,} \quad t - 1 = \frac{q-1}{2}$$

haben. Hieraus folgt unmittelbar, dass M

$$= \frac{q-1}{2} \cdot \frac{p-1}{2} - \left\{\left[\frac{p}{q}\right] + \left[\frac{2p}{q}\right] + \cdots + \left[\frac{\frac{1}{2}(q-1)p}{q}\right]\right\}$$

ist. Setzen wir daher

$$N = \left[\frac{p}{q}\right] + \left[\frac{2p}{q}\right] + \cdots + \left[\frac{\frac{1}{2}(q-1)p}{q}\right],$$

so ist

$$M + N = \frac{q-1}{2} \cdot \frac{p-1}{2},$$

wenn, wie wir vorausgesetzt haben, q eine positive ungerade Zahl und kleiner als p ist. Nun haben wir oben gesehen, dass

$$\left(\frac{q}{p}\right) = (-1)^M$$

ist; wenn daher q eine positive ungerade *Primzahl* bedeutet, so ist offenbar nach demselben Satze

$$\left(\frac{p}{q}\right) = (-1)^N$$

denn N ist nach demselben Gesetze aus q und p gebildet, wie M aus p und q. Multipliciren wir daher diese beiden Gleichungen, so erhalten wir die Gleichung

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{1}{2}(q-1)\cdot\frac{1}{2}(p-1)},$$

welche ja den Reciprocitätssatz ausspricht. Die während des Beweises gemachte Einschränkung, dass die Primzahl q kleiner sei als die Primzahl p, können wir nun natürlich wieder fallen lassen; denn da der Satz ganz symmetrisch in Bezug auf beide Primzahlen lautet, und ausserdem eine von beiden, da sie verschieden sind, doch nothwendig die kleinere sein muss, so wird der Satz immer richtig sein, auch wenn p die kleinere von beiden Primzahlen ist.

§. 45.

Wir betrachten zunächst ein Beispiel, um die Nützlichkeit des Reciprocitätssatzes für die Beurtheilung der Möglichkeit einer Congruenz von der Form

$$x^2 \equiv D \pmod{p}$$

nachzuweisen. Nehmen wir die Congruenz

$$x^2 \equiv 365 \pmod{1847},$$

so ist der Werth des Symbols

$$\left(\frac{365}{1847}\right)$$

zu ermitteln. Zunächst zerlegen wir 365 in Primfactoren, obgleich dies, wie wir später sehen werden, nicht nothwendig ist.

Aus dieser Zerlegung $365 = 5 \cdot 73$ folgt unmittelbar

$$\left(\frac{365}{1847}\right) = \left(\frac{5}{1847}\right)\left(\frac{73}{1847}\right).$$

Da ferner 5 von der Form $4n + 1$ ist, so ergiebt sich aus dem Reciprocitätssatze

$$\left(\frac{5}{1847}\right) = \left(\frac{1847}{5}\right)$$

und also, da $1847 \equiv 2 \pmod{5}$ ist,

$$\left(\frac{5}{1847}\right) = \left(\frac{2}{5}\right) = -1$$

nach §. 41; da ferner auch 73 von der Form $4n + 1$ ist, so folgt wieder aus dem Reciprocitätssatze, und weil $1847 \equiv 22 \pmod{73}$ ist,

$$\left(\frac{73}{1847}\right) = \left(\frac{1847}{73}\right) = \left(\frac{22}{73}\right) = \left(\frac{2}{73}\right)\left(\frac{11}{73}\right);$$

nun ist aber $73 \equiv 1 \pmod{8}$, also (nach §. 41)

$$\left(\frac{2}{73}\right) = 1, \quad \text{folglich } \left(\frac{73}{1847}\right) = \left(\frac{11}{73}\right);$$

nach dem Reciprocitätssatze ist aber wieder

$$\left(\frac{11}{73}\right) = \left(\frac{73}{11}\right) = \left(\frac{7}{11}\right),$$

und da beide Primzahlen 7 und 11 von der Form $4n + 3$ sind, so ist abermals nach dem Reciprocitätssatze

$$\left(\frac{7}{11}\right) = -\left(\frac{11}{7}\right) = -\left(\frac{4}{7}\right) = -1,$$

folglich

$$\left(\frac{73}{1847}\right) = \left(\frac{11}{73}\right) = \left(\frac{7}{11}\right) = -1$$

und also endlich

$$\left(\frac{365}{1847}\right) = \left(\frac{5}{1847}\right)\left(\frac{73}{1847}\right) = (-1)(-1) = +1,$$

es ist also 365 quadratischer Rest der Primzahl 1847, d. h. die oben vorgelegte Congruenz ist möglich; und in der That ist

$$(\pm 496)^2 = 246016 = 365 + 133 \cdot 1847.$$

§. 46.

Der in dem eben behandelten Beispiel angewendete Algorithmus, welcher auch bei jedem ähnlichen Beispiel nach einer endlichen Anzahl von Operationen zum Ziele führt, lässt sich im Allgemeinen bedeutend abkürzen, wenn man sich einer zuerst von *Jacobi* in die Zahlentheorie eingeführten Verallgemeinerung des Legendre'schen Symbols bedient; da der Gebrauch dieses Zeichens auch für unsere spätern Untersuchungen unerlässlich ist, so beschäftigen wir uns zunächst mit der Erklärung desselben und den Gesetzen, denen es gehorcht.

Es sei die ungerade Zahl P in ihre Primzahlfactoren p, p', p'' u. s. w. zerlegt, also

$$P = p\,p'\,p'' \ldots$$

und m irgend eine relative Primzahl zu P; so kommt es oft darauf an zu untersuchen, ob m von einer geraden oder ungeraden Anzahl der sämmtlichen Primzahlen $p, p', p'' \ldots$ quadratischer Nichtrest ist, d. h. ob das Product

$$\left(\frac{m}{p}\right)\left(\frac{m}{p'}\right)\left(\frac{m}{p''}\right) \ldots$$

$= +1$ oder $= -1$ ist; dieses Product soll nun von jetzt an mit dem einfachen Zeichen $\left(\frac{m}{P}\right)$ bezeichnet werden. Wenn m quadratischer Rest von P, und also auch von jeder einzelnen der Primzahlen $p, p', p'' \ldots$ ist, so ist

$$\left(\frac{m}{p}\right) = \left(\frac{m}{p'}\right) = \left(\frac{m}{p''}\right) \ldots = 1,$$

und folglich auch

$$\left(\frac{m}{P}\right) = \left(\frac{m}{p}\right)\left(\frac{m}{p'}\right)\left(\frac{m}{p''}\right)\cdots = 1;$$

aber man darf diesen Satz durchaus nicht umkehren; sobald nämlich die Zahl m von zweien der Primfactoren $p, p', p''\ldots$ (oder von vier, von sechs u. s. w.) quadratischer Nichtrest ist, so hat das Symbol $\left(\frac{m}{P}\right)$ den Werth $+1$, und doch ist m quadratischer Nichtrest von P. Im einfachsten Fall, wo P selbst eine ungerade Primzahl ist, stimmt die Bedeutung des Zeichens offenbar mit der früheren überein. Der Vollständigkeit wegen wollen wir ferner festsetzen, dass, wenn $P = 1$, das Zeichen $\left(\frac{m}{P}\right) = \left(\frac{m}{1}\right)$ immer die positive Einheit bedeuten soll.

Aus dieser Definition des Zeichens $\left(\frac{m}{P}\right)$ ergeben sich nun folgende Sätze:

1) Ist m relative Primzahl gegen jede der beiden ungeraden Zahlen P und Q, also auch gegen die ungerade Zahl PQ, so ist

$$\left(\frac{m}{P}\right)\left(\frac{m}{Q}\right) = \left(\frac{m}{PQ}\right);$$

denn, wenn

$$P = p\,p'\,p''\ldots$$
$$Q = q\,q'\,q''\ldots$$

ist, wo $p, p'\ldots q, q'\ldots$ lauter Primzahlen bedeuten, so ist

$$\left(\frac{m}{PQ}\right) = \left(\frac{m}{p}\right)\left(\frac{m}{p'}\right)\left(\frac{m}{p''}\right)\cdots\left(\frac{m}{q}\right)\left(\frac{m}{q'}\right)\left(\frac{m}{q''}\right)\cdots$$
$$= \left(\frac{m}{P}\right)\left(\frac{m}{Q}\right).$$

2) Sind die Zahlen $l, m, n\ldots$ relative Primzahlen gegen die ungerade Zahl P, so ist

$$\left(\frac{l}{P}\right)\left(\frac{m}{P}\right)\left(\frac{n}{P}\right)\cdots = \left(\frac{l\,m\,n\ldots}{P}\right);$$

denn, wenn wieder

$$P = p\,p'\,p''\ldots$$

ist, so ist

$$\left(\frac{l}{P}\right) = \left(\frac{l}{p}\right)\left(\frac{l}{p'}\right)\left(\frac{l}{p''}\right)\cdots$$

$$\left(\frac{m}{P}\right) = \left(\frac{m}{p}\right)\left(\frac{m}{p'}\right)\left(\frac{m}{p''}\right)\cdots$$

$$\left(\frac{n}{P}\right) = \left(\frac{n}{p}\right)\left(\frac{n}{p'}\right)\left(\frac{n}{p''}\right)\cdots$$

u. s. w.

Da nun ferner, wie früher (§. 33) bewiesen ist,

$$\left(\frac{l}{p}\right)\left(\frac{m}{p}\right)\left(\frac{n}{p}\right)\cdots = \left(\frac{l\,m\,n\ldots}{p}\right)$$

ist und Aehnliches für die andern Primfactoren p', p'' u. s. w. gilt, so erhält man durch Multiplication der vorangehenden Gleichungen

$$\left(\frac{l}{P}\right)\left(\frac{m}{P}\right)\left(\frac{n}{P}\right)\cdots = \left(\frac{l\,m\,n\ldots}{p}\right)\left(\frac{l\,m\,n\ldots}{p'}\right)\left(\frac{l\,m\,n\ldots}{p''}\right)\cdots,$$

worin der zu beweisende Satz besteht.

3) Ist m relative Primzahl zu der ungeraden Zahl P und $m \equiv m'$ (mod. P), also auch m' relative Primzahl zu P, so ist

$$\left(\frac{m}{P}\right) = \left(\frac{m'}{P}\right);$$

denn, wenn $P = p\;p'\;p''\ldots$ ist, so ist auch

$$m \equiv m' \text{ (mod. } p\text{)},\quad m \equiv m' \text{ (mod. } p'\text{)},$$

u. s. w., also

$$\left(\frac{m}{p}\right) = \left(\frac{m'}{p}\right),\; \left(\frac{m}{p'}\right) = \left(\frac{m'}{p'}\right),$$

u. s. w., und folglich

$$\left(\frac{m}{p}\right)\left(\frac{m}{p'}\right)\cdots = \left(\frac{m'}{p}\right)\left(\frac{m'}{p'}\right)\cdots,$$

was zu beweisen war. —

Die beiden letzten Sätze zeigen, dass das verallgemeinerte Symbol denselben Gesetzen gehorcht wie das einfache; wir wollen

nun zeigen, dass auch die Werthe der Symbole $\left(\frac{-1}{P}\right)$, $\left(\frac{2}{P}\right)$ nach den frühern Regeln zu bestimmen sind, und endlich, dass auch ein dem frühern ganz analoger Reciprocitätssatz Statt findet; um aber den Gang der Beweise nicht zu unterbrechen, schicken wir folgende Bemerkungen voraus. Ist

$$R = r' \, r'' \, r''' \ldots$$

eine beliebige ungerade Zahl, so sind $r'-1$, $r''-1$, $r'''-1 \ldots$ lauter gerade Zahlen, und folglich ist jedes Product aus zweien oder mehreren dieser Differenzen $\equiv 0 \pmod{4}$; bringt man daher R in die Form

$$R = (1 + (r'-1))\,(1 + (r''-1))\,(1 + (r''-1)) \ldots$$

und führt die Multiplication aus, so ergiebt sich

$$R \equiv 1 + (r'-1) + (r''-1) + (r'''-1) + \ldots \pmod{4}$$

oder kürzer

$$\frac{R-1}{2} \equiv \Sigma \, \frac{r-1}{2} \pmod{2},$$

wo das Summenzeichen sich auf den Buchstaben r bezieht, der die einzelnen Factoren r', r'', r''' ... durchlaufen muss.

Auf ganz ähnliche Weise ergiebt sich aus denselben Voraussetzungen noch ein zweites Lemma; es ist nämlich $r^2 \equiv 1 \pmod{8}$ und folglich

$$R^2 = (1 + (r'^2-1))\,(1 + (r''^2-1))\,(1 + (r'''^2-1)) \ldots$$
$$\equiv 1 + \Sigma\,(r^2 - 1) \pmod{64},$$

also

$$\frac{R^2-1}{8} \equiv \Sigma \, \frac{r^2-1}{8} \pmod{8}$$

und um so mehr

$$\frac{R^2-1}{8} \equiv \Sigma \, \frac{r^2-1}{8} \pmod{2}.$$

Nach diesen Vorbemerkungen kehren wir zu unserm Gegenstande zurück.

4) Ist P eine positive ungerade Zahl, so ist

$$\left(\frac{-1}{P}\right) = (-1)^{\frac{P-1}{2}}.$$

Denn wenn P das Product aus den positiven Primzahlen p', p'', p''' ... ist, so ist

$$\left(\frac{-1}{P}\right) = \left(\frac{-1}{p'}\right)\left(\frac{-1}{p''}\right)\left(\frac{-1}{p'''}\right)\cdots = (-1)^{\Sigma\frac{p-1}{2}},$$

wo der Summationsbuchstabe p alle Primfactoren p', p'', p''' ... durchlaufen muss; da nun nach dem ersten Lemma

$$\Sigma\,\frac{p-1}{2} \equiv \frac{P-1}{2} \pmod{2}$$

ist, so leuchtet die Richtigkeit des Satzes ein.

5) Ist P eine ungerade Zahl, so ist

$$\left(\frac{2}{P}\right) = (-1)^{\frac{P^2-1}{8}}.$$

Denn mit Beibehaltung derselben Zeichen ist

$$\left(\frac{2}{P}\right) = \left(\frac{2}{p'}\right)\left(\frac{2}{p''}\right)\left(\frac{2}{p'''}\right)\cdots = (-1)^{\Sigma\frac{p^2-1}{8}},$$

und da nach dem zweiten Lemma

$$\Sigma\,\frac{p^2-1}{8} \equiv \frac{P^2-1}{8} \pmod{2}$$

ist, so ergiebt sich unmittelbar die Richtigkeit des zu beweisenden Satzes.

6) Sind die beiden positiven ungeraden Zahlen P und Q relative Primzahlen zu einander, so ist

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}.$$

Denn es sei P das Product aus den Primzahlen

$$p',\ p'',\ p''' \ldots \qquad (p)$$

und Q das Product aus den Primzahlen

$$q',\ q'' \ldots \qquad (q)$$

welche also von den Primzahlen p', p'', p''' ... verschieden sind. Dann ist zufolge der Erklärung und nach 2)

$$\left(\frac{P}{Q}\right) = \left(\frac{P}{q'}\right)\left(\frac{P}{q''}\right)\cdots = \Pi\left(\frac{p}{q}\right),$$

wo das Productzeichen Π sich auf alle Combinationen einer jeden der Primzahlen p mit einer jeden der Primzahlen q bezieht; ganz ebenso ist aber

$$\left(\frac{Q}{P}\right) = \Pi\left(\frac{q}{p}\right)$$

und folglich

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = \Pi\left(\frac{p}{q}\right)\left(\frac{q}{p}\right),$$

wo das Productzeichen sich auf dieselben Combinationen bezieht; da nun nach dem Reciprocitätssatze

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

ist, so ergiebt sich

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{\Sigma\frac{p-1}{2}\cdot\frac{q-1}{2}},$$

wo wieder das Summenzeichen sich auf dieselben Combinationen jeder Primzahl p mit jeder Primzahl q erstreckt; es ist daher

$$\Sigma\frac{p-1}{2}\,\frac{q-1}{2} = \Sigma\frac{p-1}{2}\times\Sigma\frac{q-1}{2},$$

wo auf der rechten Seite das erste Summenzeichen sich auf alle Primzahlen p, das zweite sich auf alle Primzahlen q bezieht. Da nun nach dem ersten Lemma

$$\Sigma\frac{p-1}{2} \equiv \frac{P-1}{2} \pmod{2}$$

und

$$\Sigma\frac{q-1}{2} \equiv \frac{Q-1}{2} \pmod{2}$$

ist, so ergiebt sich

$$\Sigma\frac{p-1}{2}\,\frac{q-1}{2} \equiv \frac{P-1}{2}\,\frac{Q-1}{2} \pmod{2}$$

und hieraus

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2}\,\frac{Q-1}{2}},$$

was zu beweisen war. —

Es bleibt uns nun noch eine Bemerkung über das Symbol $\left(\frac{m}{P}\right)$ zu machen übrig; wir haben bisher dieses Zeichen nur unter der Voraussetzung definirt, dass die Zahl P eine positive ungerade Zahl, und dass die positive oder negative Zahl m relative Primzahl zu P ist; wir erweitern jetzt die Bedeutung des Zeichens dahin, dass P auch eine negative ungerade Zahl sein kann, immer aber mit der Beschränkung, dass m relative Primzahl zu P ist*); und zwar setzen wir fest, dass

$$\left(\frac{m}{-P}\right) = \left(\frac{m}{P}\right)$$

sein soll. Dann leuchtet augenblicklich ein, dass die Sätze 1), 2), 3) und 5) ohne Beschränkung gültig bleiben; ferner, dass der Satz 4) nur dann richtig ist, wenn P positiv ist, dagegen für ein negatives P falsch wird; und endlich, dass der Satz 6) nur dann gültig bleibt, wenn mindestens eine der beiden Zahlen P und Q positiv ist, dagegen seine Gültigkeit verliert, wenn beide Zahlen P und Q negativ sind.

§. 47.

Die oben (§. 45) an einem Beispiel behandelte Aufgabe, den Werth des Symbols $\left(\frac{m}{p}\right)$ zu bestimmen, wenn p eine ungerade Primzahl ist, bildet offenbar nur einen ganz speciellen Fall der allgemeinen Aufgabe, den Werth irgend eines Symbols $\left(\frac{m}{P}\right)$ zu bestimmen; damals war, nachdem m auf seinen kleinsten Rest

*) Später (Supplemente §. 116) werden wir festsetzen, dass $\left(\frac{m}{P}\right) = 0$ sein soll, sobald P eine ungerade Zahl, m aber keine relative Primzahl zu P ist.

nach dem Modul p reducirt war, der nächste Schritt der, m in seine Primfactoren q, q' u. s. w. zu zerlegen, und dann, die einzelnen Symbole $\left(\frac{q}{p}\right)$, $\left(\frac{q'}{p}\right)$ u. s. w. mit Hülfe des Reciprocitätssatzes in einfachere umzuformen. Jetzt ist diese Zerlegung in Primzahlfactoren (abgesehen von dem Factor 2) ganz überflüssig geworden, und der anzuwendende Algorithmus ist demjenigen ganz ähnlich, durch welchen der grösste gemeinschaftliche Divisor zweier Zahlen gefunden wird. Einige Beispiele werden genügen, um diese einfachere Methode zu erläutern.

Beispiel 1: Nehmen wir das schon oben (§. 45) behandelte Beispiel, so können wir jetzt nach dem verallgemeinerten Reciprocitätssatze

$$\left(\frac{365}{1847}\right) = \left(\frac{1847}{365}\right)$$

setzen, weil 365 von der Form $4n+1$ ist. Da ferner $1847 \equiv 22$ (mod. 365) ist, so ist nach §. 46, 3) und 2)

$$\left(\frac{1847}{365}\right) = \left(\frac{22}{365}\right) = \left(\frac{2}{365}\right)\left(\frac{11}{365}\right);$$

da ferner $365 \equiv 5$ (mod. 8), so ist nach §. 46, 5)

$$\left(\frac{2}{365}\right) = -1,$$

also

$$\left(\frac{365}{1847}\right) = -\left(\frac{11}{365}\right).$$

Nach dem verallgemeinerten Reciprocitätssatze ist nun wieder

$$\left(\frac{11}{365}\right) = \left(\frac{365}{11}\right) = \left(\frac{2}{11}\right) = -1,$$

und folglich

$$\left(\frac{365}{1847}\right) = +1,$$

wie früher.

Beispiel 2: Nach dem verallgemeinerten Reciprocitätssatze ist

$$\left(\frac{195}{1901}\right) = \left(\frac{1901}{195}\right);$$

weil $1901 \equiv -49 \pmod{195}$, so ist

$$\left(\frac{1901}{195}\right) = \left(\frac{-49}{195}\right);$$

da ferner die Zahlen -49 und 195 nicht beide negativ sind, so gilt für sie der verallgemeinerte Reciprocitätssatz, und, weil beide von der Form $4n+3$ sind, so ist

$$\left(\frac{-49}{195}\right) = -\left(\frac{195}{-49}\right) = -\left(\frac{195}{49}\right);$$

weil endlich $195 \equiv -1 \pmod{49}$, und 49 von der Form $4n+1$ ist, so ist

$$\left(\frac{195}{49}\right) = \left(\frac{-1}{49}\right) = +1,$$

also

$$\left(\frac{195}{1901}\right) = -1$$

d. h. 195 ist quadratischer Nichtrest der Primzahl 1901. Natürlich hätte sich die Auflösung abkürzen lassen durch Zerlegung in Factoren, nämlich durch die Bemerkung, dass $49 = 7 \cdot 7$ und folglich

$$\left(\frac{-49}{195}\right) = \left(\frac{-1}{195}\right) = -1$$

ist; überhaupt wird die Operation immer bedeutend abgekürzt, wenn man im Zähler oder Nenner des Symbols quadratische Factoren bemerkt, da diese sogleich fortgelassen werden können.

Beispiel 3: Um den Werth des Symbols $\left(\frac{74}{101}\right)$ zu bestimmen, kann man zuerst aus dem Zähler den Factor 2 absondern, wodurch man, da 101 von der Form $8n+5$ ist,

$$\left(\frac{74}{101}\right) = \left(\frac{2}{101}\right)\left(\frac{37}{101}\right) = -\left(\frac{37}{101}\right)$$

erhält; dann ist ferner nach dem Reciprocitätssatze

$$\left(\frac{37}{101}\right) = \left(\frac{101}{37}\right) = \left(\frac{-10}{37}\right) = \left(\frac{10}{37}\right)$$

und, weil 37 von der Form $8n+5$ ist,

$$\left(\frac{10}{37}\right) = \left(\frac{2}{37}\right)\left(\frac{5}{37}\right) = -\left(\frac{5}{37}\right);$$

endlich ist wieder nach dem Reciprocitätssatze

$$\left(\frac{5}{37}\right) = \left(\frac{37}{5}\right) = \left(\frac{2}{5}\right) = -1$$

und folglich

$$\left(\frac{74}{101}\right) = -1.$$

Kürzer gelangt man durch folgende Kette zum Ziele:

$$\left(\frac{74}{101}\right) = \left(\frac{-27}{101}\right) = \left(\frac{101}{-27}\right) = \left(\frac{-7}{27}\right) = \left(\frac{27}{-7}\right) = \left(\frac{-1}{7}\right)$$
$$= -1.$$

§. 48.

Wegen der Wichtigkeit des Reciprocitätssatzes theilen wir hier noch einen andern Beweis desselben mit, nämlich den ersten der von *Gauss* gegebenen sechs Beweise*); dies kann hier um so eher geschehen, als durch die im Vorhergehenden erörterte Verallgemeinerung des Legendre'schen Symbols mehrere der von *Gauss* unterschiedenen acht Fälle sich zusammenziehen lassen, wodurch der Beweis an Kürze und Uebersichtlichkeit bedeutend gewinnt**).

Das Wesen dieses Beweises besteht in der sogenannten vollständigen Induction; wenn nämlich der Satz für je zwei Primzahlen p, p' richtig ist, welche kleiner sind, als eine bestimmte Primzahl q, so lässt sich zeigen, dass er auch für jede Combination einer solchen Primzahl p mit der Primzahl q selbst gelten muss; hieraus und weil der Satz für die beiden kleinsten ungeraden Primzahlen 3 und 5 wirklich richtig ist, folgt dann unmittelbar seine Allgemeingültigkeit.

---

*) *Disquisitiones Arithmeticae* artt. 135 — 144.

**) *Dirichlet: Ueber den ersten der von Gauss gegebenen Beweise des Reciprocitätsgesetzes in der Theorie der quadratischen Reste* (Crelle's Journal XLVII).

Von besonderer Wichtigkeit für diesen Nachweis ist nun die vorläufige Bemerkung, dass aus der angenommenen Richtigkeit des Reciprocitätssatzes für je zwei Primzahlen p, p', welche kleiner als die Primzahl q sind, mit Nothwendigkeit auch die Gültigkeit des verallgemeinerten Satzes

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2}\,\frac{Q-1}{2}}$$

folgt, sobald die beiden ungeraden relativen Primzahlen P und Q (die nicht gleichzeitig negativ sein dürfen) nur solche Primzahlfactoren enthalten, die kleiner als q sind; denn der Beweis dieses verallgemeinerten Satzes gründete sich ausschliesslich auf die Richtigkeit des einfachen Satzes für alle die Paare von zwei Primzahlen, von denen die eine in P, die andere in Q aufgeht.

Eine letzte vorläufige Bemerkung, welche mehrere Male zur Anwendung kommen wird, ist folgende: ist jede der beiden Zahlen k und l relative Primzahl gegen die ungerade Zahl m, und ist die Congruenz $kx^2 \equiv l$ (mod. m) möglich, so ist immer $\left(\frac{k}{m}\right) = \left(\frac{l}{m}\right)$; denn kl ist quadratischer Rest von m, und folglich

$$\left(\frac{kl}{m}\right) = \left(\frac{k}{m}\right)\left(\frac{l}{m}\right) = 1.$$

Bei dem Beweise nun, dass der Reciprocitätssatz für jede Combination von q mit einer Primzahl p, welche kleiner als q ist, gilt, haben wir zwei Fälle zu unterscheiden. Der eine Fall und zwar der schwierigere findet Statt, wenn q die Form $4n + 1$ hat, und zugleich p quadratischer Nichtrest von q ist; dann ist zu beweisen, dass auch q quadratischer Nichtrest von p ist. In irgend einem der andern Fälle, nämlich wenn q von der Form $4n + 3$ ist, oder auch, wenn q zwar die Form $4n + 1$ hat, dann aber p quadratischer Rest von q ist, kann man offenbar der Primzahl p immer ein solches Vorzeichen geben, dass, wenn man $\omega = \pm p$ setzt, wenigstens für eins der beiden Vorzeichen ω quadratischer Rest von q wird; dann ist also zu beweisen, dass

$$\left(\frac{q}{\omega}\right) = (-1)^{\frac{1}{2}(\omega-1)\cdot\frac{1}{2}(q-1)}$$

ist; dieser letztere Fall ist deshalb leichter zu behandeln, weil die Annahme sogleich einen Ansatz giebt, welcher nur ausgebeutet zu werden braucht. Wir beginnen daher mit diesem Theil des Satzes.

§. 49.

Es sei also $\omega = \pm p$ quadratischer Rest von q, so hat die Congruenz $x^2 \equiv \omega \pmod{q}$ zwischen 0 und q immer zwei Wurzeln x, deren Summe $= q$, und von denen folglich die eine, welche wir mit e bezeichnen wollen, eine gerade Zahl ist. Dann wird

$$e^2 - \omega = qf$$

sein, wo f eine ganze Zahl bedeutet, welche jedenfalls nicht $= 0$ ist, weil sonst die Primzahl ω eine Quadratzahl sein müsste. Diese Zahl f kann aber auch nicht negativ sein; denn sonst wäre ω positiv $= p$, und $p - e^2$ eine positive durch q theilbare Zahl, was aber unmöglich ist, da $p - e^2 < p$ und der Voraussetzung nach $p < q$ ist. Diese positive Zahl f muss ferner ungerade sein; denn da e gerade ist, so ist $e^2 - \omega$ ungerade, und folglich auch jeder Divisor von $e^2 - \omega$, also auch f ungerade. Endlich ist diese positive ungerade Zahl f nothwendig $< q - 1$; denn da $e \leqq q - 1$, und $p < q - 1$, so ist $qf = e^2 - \omega < (q-1)^2 + (q-1)$, d. h. $qf < q(q-1)$, also wirklich $f < q - 1$.

Nun sind zwei Fälle möglich:

1) Ist f nicht durch p theilbar, so folgt aus der Gleichung $e^2 - \omega = qf$, dass

$$\left(\frac{\omega}{f}\right) = +1,$$

und ferner, weil qf quadratischer Rest von p ist, dass

$$\left(\frac{q}{\omega}\right) = \left(\frac{f}{\omega}\right)$$

sein muss; da nun die beiden ungeraden Zahlen f und ω relative Primzahlen zu einander, beide kleiner als q, und endlich nicht beide negativ sind, so gilt für sie der verallgemeinerte Reciprocitätssatz, d. h. es ist

$$\left(\frac{f}{\omega}\right)\left(\frac{\omega}{f}\right) = (-1)^{\frac{1}{2}(\omega-1)\cdot\frac{1}{2}(f-1)}$$

und hieraus ergiebt sich unter Berücksichtigung der beiden vorhergehenden Gleichungen

$$\left(\frac{q}{\omega}\right) = (-1)^{\frac{1}{2}(\omega-1)\cdot\frac{1}{2}(f-1)}.$$

Da ferner e eine gerade Zahl ist, so ist auch $-\omega \equiv qf \pmod{4}$, also (nach dem ersten Lemma in §. 46)

$$-\frac{\omega+1}{2} \equiv \frac{qf-1}{2} \equiv \frac{q-1}{2} + \frac{f-1}{2} \pmod{2};$$

multiplicirt man diese Congruenz mit $\frac{1}{2}(\omega-1)$, so erhält man auf der linken Seite ein Product aus zwei successiven ganzen Zahlen, also gewiss eine gerade Zahl, und hieraus folgt unmittelbar

$$\frac{\omega-1}{2}\,\frac{f-1}{2} \equiv \frac{\omega-1}{2}\,\frac{q-1}{2} \pmod{2}$$

und also

$$\left(\frac{q}{\omega}\right) = (-1)^{\frac{1}{2}(\omega-1)\cdot\frac{1}{2}(q-1)},$$

was zu beweisen war.

2) Ist dagegen f theilbar durch p, so kann man $f = \omega\varphi$ setzen, wo φ eine ungerade Zahl bedeutet, die dasselbe Zeichen wie ω hat und ihrem absoluten Werthe nach $< q$ ist. Da nun $e^2 - \omega = q\omega\varphi$, so ist auch e theilbar durch ω und also $e = \varepsilon\omega$, wo ε wieder eine gerade Zahl ist. Hieraus ergiebt sich nun

$$\varepsilon^2\omega - 1 = q\varphi,$$

und es kann daher φ nicht durch ω theilbar sein. Nun war ω quadratischer Rest von $f = \omega\varphi$, und folglich auch von φ, also ist

$$\left(\frac{\omega}{\varphi}\right) = \left(\frac{\omega}{-\varphi}\right) = +1;$$

ausserdem folgt aus der vorhergehenden Gleichung, dass $-q\varphi$ quadratischer Rest von ω, dass also

$$\left(\frac{q}{\omega}\right) = \left(\frac{-\varphi}{\omega}\right)$$

ist; da endlich von den beiden ungeraden Zahlen $-\varphi$ und ω die eine positiv ist, und da sie relative Primzahlen zu einander und ausserdem beide $< q$ sind, so ist nach dem verallgemeinerten Reciprocitätssatze

$$\left(\frac{-\varphi}{\omega}\right)\left(\frac{\omega}{-\varphi}\right) = (-1)^{\frac{1}{2}(\omega-1)\cdot\frac{1}{2}(\varphi+1)}$$

und folglich unter Berücksichtigung der beiden vorhergehenden Gleichungen

$$\left(\frac{q}{\omega}\right) = (-1)^{\frac{1}{2}(\omega-1)\cdot\frac{1}{2}(\varphi+1)}.$$

Da nun ε eine gerade Zahl und folglich $q\varphi \equiv -1 \pmod{4}$ ist, so muss die eine der beiden Zahlen φ und q von der Form $4n+1$, die andere aber von der Form $4n+3$ sein, woraus folgt, dass

$$\frac{\varphi+1}{2} \equiv \frac{q-1}{2} \pmod{2}$$

und also

$$\left(\frac{q}{\omega}\right) = (-1)^{\frac{1}{2}(\omega-1)\cdot\frac{1}{2}(q-1)}$$

ist. Also ist auch für diesen Fall der Satz bewiesen.

§. 50.

Wir kommen nun zu dem zweiten Theil, in welchem vorausgesetzt wird, dass p Nichtrest von q, und q von der Form $4n+1$ ist, und in welchem bewiesen werden muss, dass q Nichtrest von p ist. Hier fehlt nun die Möglichkeit eines Ansatzes, und um diese zu gewinnen, kommt alles darauf an nachzuweisen, dass wenigstens eine Primzahl $p' < q$ existirt, von welcher q quadratischer Nichtrest ist, oder mit andern Worten, dass die Prim-

zahl q nicht von allen kleinern Primzahlen quadratischer Rest sein kann. Für den Fall, dass $q \equiv 5 \pmod{8}$ ist, hat dieser Nachweis nicht die geringste Schwierigkeit; denn dann ist $\frac{1}{2}(q+1) \equiv 3 \pmod{4}$, und folglich muss unter den Primfactoren dieser Zahl $\frac{1}{2}(q+1)$, welche natürlich alle $< q$ sind, mindestens einer p' von der Form $4n+3$ sein; dann ist aber $q \equiv -1 \pmod{p'}$ und folglich quadratischer Nichtrest einer kleinern Primzahl p'. Desto schwieriger war dieser Nachweis für den andern Fall zu führen, in welchem $q \equiv 1 \pmod{8}$ ist; und *Gauss* selbst gesteht *), dass es ihm erst nach manchen vergeblichen Versuchen gelungen ist, diese capitale Schwierigkeit zu überwinden; er gelangte dazu durch folgende äusserst scharfsinnige Betrachtung.

Es sei $2m+1$ irgend eine ungerade Zahl, aber kleiner als q. Wenn nun q quadratischer Rest von allen ungeraden Primzahlen z ist, welche diese ungerade Zahl $2m+1$ nicht übertreffen, so ist nach frühern Sätzen (§. 37) die Primzahl q, da sie $\equiv 1 \pmod{8}$ und also von jeder Potenz der Zahl 2 quadratischer Rest ist, auch quadratischer Rest von jeder Zahl, welche keine andern ungeraden Primfactoren als die Primzahlen z enthält, und also z. B. von der Zahl

$$M = 1 \cdot 2 \cdot 3 \cdot 4 \ldots\ldots (2m)\ (2m+1);$$

es giebt daher positive Zahlen k von der Beschaffenheit, dass

$$q \equiv k^2 \pmod{M}$$

ist, und zwar muss k relative Primzahl zu M sein, weil $2m+1 < q$ und also auch q relative Primzahl zu M ist. Aus dieser Congruenz folgt nun weiter, dass in Bezug auf den Modul M

$$\begin{aligned} & k\,(q-1^2)\,(q-2^2)\,(q-3^2)\ldots(q-m^2) \\ \equiv\ & k\,(k^2-1^2)\,(k^2-2^2)\,(k^2-3^2)\ldots(k^2-m^2) \\ \equiv\ & (k+m)\,(k+m-1)\ldots(k+1)\,k\,(k-1)\ldots(k-m+1)\,(k-m) \end{aligned}$$

ist; da nun nach einem frühern Satze (§. 15 Anmerkung) jedes Product von $(2m+1)$ successiven ganzen Zahlen durch M theil-

*) *Disquisitiones Arithmeticae* art. 125.

bar, und ausserdem k relative Primzahl zu M ist, so ist das Product

$$(q - 1^2)\ (q - 2^2)\ (q - 3^2) \ldots (q - m^2)$$

theilbar durch das Product

$$M = (m + 1)\ ((m + 1)^2 - 1^2)\ ((m + 1)^2 - 2^2) \ldots ((m + 1)^2 - m^2)$$

d. h. das Product

$$\frac{1}{m+1} \cdot \frac{q - 1^2}{(m+1)^2 - 1^2} \cdot \frac{q - 2^2}{(m+1)^2 - 2^2} \cdots \frac{q - m^2}{(m+1)^2 - m^2}$$

ist nothwendig eine ganze Zahl.

Andererseits leuchtet ein, dass dieses Product gewiss keine ganze Zahl ist, sobald für m die grösste ganze Zahl unterhalb $\sqrt{q}$ genommen wird; denn, wenn $m < \sqrt{q} < m + 1$ ist, so sind alle Factoren dieses Productes echte Brüche. Da nun ausserdem $2m + 1 < 2\sqrt{q} + 1 < q$ ist, so kann für diese Zahl m die Annahme nicht zulässig sein, und wir haben daher folgenden Satz gewonnen:

Ist q eine Primzahl von der Form $8n + 1$, so giebt es unterhalb $2\sqrt{q} + 1$ und folglich auch unterhalb q mindestens eine ungerade Primzahl p', von welcher q quadratischer Nichtrest ist.

§. 51.

Nachdem für jede Primzahl q von der Form $4n + 1$ die Existenz einer Primzahl $p' < q$ nachgewiesen ist, von welcher q quadratischer Nichtrest ist, gehen wir zum Beweise unseres zweiten Theiles über. Jede solche Primzahl p' muss Nichtrest von q sein; denn wäre p' Rest von q, so würde aus dem schon von uns bewiesenen Theil (§. 49)

$$\left(\frac{q}{p'}\right) = (-1)^{\frac{1}{2}(p'-1) \cdot \frac{1}{2}(q-1)} = +1$$

folgen, was mit der Voraussetzung streitet. Mithin gilt für diese Primzahl p' das Reciprocitätsgesetz. Giebt es nun *ausser* p' noch

andere ungerade Primzahlen $p < q$, welche Nichtreste von q sind, so ist nur zu beweisen, dass

$$\left(\frac{q}{pp'}\right) = +1$$

ist, weil hieraus sogleich folgt, dass q Nichtrest von p ist. Da nun der Voraussetzung nach p' und p quadratische Nichtreste von q sind, so ist pp' quadratischer Rest von q, und es giebt daher wieder eine gerade Zahl $e < q$ von der Beschaffenheit, dass

$$e^2 - pp' = q\varphi$$

und φ eine ganze Zahl ist; und weil die linke Seite dieser Gleichung eine ungerade Zahl darstellt, welche ihrem absoluten Werthe nach $< q^2$ ist, so ist φ ebenfalls eine ungerade Zahl und zwar $< q$. Je nach der Beschaffenheit dieser Zahl φ zerfällt nun der Beweis in drei Theile.

1) Ist φ weder durch p noch durch p' theilbar, so ist

$$\left(\frac{pp'}{\varphi}\right) = +1,$$

und da $q\varphi$ quadratischer Rest von pp' ist, auch

$$\left(\frac{q\varphi}{pp'}\right) = 1, \text{ also } \left(\frac{q}{pp'}\right) = \left(\frac{\varphi}{pp'}\right);$$

da ferner die beiden ungeraden relativen Primzahlen φ und pp' (von denen die letztere positiv ist) nur solche Primfactoren enthalten, welche $< q$ sind, so gilt für diese beiden Zahlen auch das verallgemeinerte Reciprocitätsgesetz, d. h. es ist

$$\left(\frac{\varphi}{pp'}\right)\left(\frac{pp'}{\varphi}\right) = (-1)^{\frac{1}{2}(\varphi-1)\cdot\frac{1}{2}(pp'-1)}$$

und folglich, mit Berücksichtigung der beiden vorhergehenden Gleichungen

$$\left(\frac{q}{pp'}\right) = (-1)^{\frac{1}{2}(\varphi-1)\cdot\frac{1}{2}(pp'-1)}.$$

Da aber e eine gerade Zahl, so ist $q\varphi \equiv -pp' \pmod{4}$, also, da $q \equiv 1 \pmod{4}$ ist,

$$\varphi \equiv -pp' \pmod{4}$$

$$\frac{\varphi - 1}{2} \equiv -\frac{pp' + 1}{2} \pmod{2}$$

also

$$\frac{\varphi - 1}{2} \cdot \frac{pp' - 1}{2} \equiv 0 \pmod{2}$$

und folglich

$$\left(\frac{q}{pp'}\right) = 1,$$

was zu beweisen war.

2) Ist φ durch p' theilbar, durch p nicht theilbar, so setze man $\varphi = p'\psi$, und, da auch e durch p' theilbar sein muss, $e = p'\varepsilon$; dann ist $\psi < q$ eine durch p nicht theilbare ungerade, und ε eine gerade Zahl, und es wird

$$p'\varepsilon^2 - p = q\psi.$$

Hieraus folgt nun zunächst wieder (da ψ relative Primzahl zu pp' ist)

$$\left(\frac{pp'}{\psi}\right) = +1,$$

ferner

$$\left(\frac{q\psi}{p}\right) = \left(\frac{p'}{p}\right), \quad \text{also} \quad \left(\frac{q}{p}\right) = \left(\frac{p'}{p}\right)\left(\frac{\psi}{p}\right)$$

und

$$\left(\frac{q\psi}{p'}\right) = \left(\frac{-p}{p'}\right), \quad \text{also} \quad \left(\frac{q}{p'}\right) = \left(\frac{-p}{p'}\right)\left(\frac{\psi}{p'}\right)$$

und folglich

$$\left(\frac{q}{pp'}\right) = \left(\frac{p'}{-p}\right)\left(\frac{-p}{p'}\right)\left(\frac{\psi}{pp'}\right) = (-1)^{\frac{1}{2}(p+1)\cdot\frac{1}{2}(p'-1)}\left(\frac{\psi}{pp'}\right);$$

da endlich ψ und pp' nur solche Primfactoren enthalten, die $< q$ sind, so ist nach dem verallgemeinerten Reciprocitätssatz

$$\left(\frac{\psi}{pp'}\right)\left(\frac{pp'}{\psi}\right) = (-1)^{\frac{1}{2}(\psi-1)\cdot\frac{1}{2}(pp'-1)}$$

und hieraus in Verbindung mit zwei vorhergehenden Gleichungen

$$\left(\frac{q}{pp'}\right) = (-1)^{\frac{1}{2}(p+1)\cdot\frac{1}{2}(p'-1)+\frac{1}{2}(\psi-1)\cdot\frac{1}{2}(pp'-1)}.$$

Da nun $\varepsilon^2 \equiv 0 \pmod{4}$ und $q \equiv 1 \pmod{4}$, so ist $\psi \equiv -p \pmod{4}$, folglich

$$\tfrac{1}{2}(\psi - 1) \equiv \tfrac{1}{2}(p + 1) \pmod{2},$$

also

$$\tfrac{1}{2}(p + 1)\cdot\tfrac{1}{2}(p' - 1) + \tfrac{1}{2}(\psi - 1)\cdot\tfrac{1}{2}(pp' - 1)$$
$$\equiv \tfrac{1}{2}(p + 1)\,[\tfrac{1}{2}(p' - 1) + \tfrac{1}{2}(pp' - 1)] \pmod{2},$$

und da ferner (nach dem ersten Lemma in §. 46)

$$\tfrac{1}{2}(pp' - 1) \equiv \tfrac{1}{2}(p - 1) + \tfrac{1}{2}(p' - 1) \pmod{2}$$

ist, so ergiebt sich

$$\tfrac{1}{2}(p + 1)\cdot\tfrac{1}{2}(p' - 1) + \tfrac{1}{2}(\psi - 1)\cdot\tfrac{1}{2}(pp' - 1)$$
$$\equiv \tfrac{1}{2}(p + 1)\cdot\tfrac{1}{2}(p - 1) \equiv 0 \pmod{2}$$

und folglich

$$\left(\frac{q}{pp'}\right) = 1,$$

was zu beweisen war.

Da bei diesem Beweise die Annahme $\left(\frac{q}{p'}\right) = -1$ gar nicht zur Anwendung gekommen ist, so wird durch einfache Vertauschung von p mit p' der Beweis für den Fall entstehen, dass φ durch p theilbar, durch p' nicht theilbar ist; denn im Uebrigen sind sowohl die Voraussetzungen als auch das zu beweisende Resultat $\left(\frac{q}{pp'}\right) = 1$ vollständig symmetrisch in Bezug auf beide Primzahlen p und p'.

3) Ist φ sowohl durch p als auch durch p' und folglich (da p und p' verschiedene Primzahlen sind) auch durch pp' theilbar, so setze man $\varphi = pp'\psi$, und, da e dann ebenfalls durch pp' theilbar ist, $e = pp'\varepsilon$; dann bedeutet ψ eine ungerade Zahl $< q$, und ε eine gerade Zahl, und es wird

$$pp'\varepsilon^2 - 1 = q\psi.$$

Hieraus folgt, dass pp' relative Primzahl zu ψ und ausserdem quadratischer Rest von ψ, also

$$\left(\frac{pp'}{\psi}\right) = +1$$

ist; ebenso ergiebt sich aber, dass $-q\psi$ quadratischer Rest von pp', dass also

$$\left(\frac{q}{pp'}\right) = \left(\frac{-\psi}{pp'}\right)$$

ist; nach dem verallgemeinerten Reciprocitätssatze, welcher offenbar für die beiden Zahlen $-\psi$ und pp' gilt, ist ferner

$$\left(\frac{-\psi}{pp'}\right)\left(\frac{pp'}{-\psi}\right) = (-1)^{\frac{1}{2}(pp'-1)\cdot\frac{1}{2}(\psi+1)},$$

und hieraus ergiebt sich in Verbindung mit den beiden vorhergehenden Gleichungen

$$\left(\frac{q}{pp'}\right) = (-1)^{\frac{1}{2}(pp'-1)\cdot\frac{1}{2}(\psi+1)}.$$

Da aber ε eine gerade Zahl, und $q \equiv 1 \pmod{4}$, so ist $\psi \equiv -1 \pmod{4}$, also $\frac{1}{2}(\psi+1)$ eine gerade Zahl, und folglich

$$\left(\frac{q}{pp'}\right) = 1,$$

was zu beweisen war.

Hiermit ist nun auch der zweite Theil des Beweises vollständig geführt und dadurch die Allgemeingültigkeit des Reciprocitätssatzes von Neuem nachgewiesen (ein dritter Beweis findet sich in den Supplementen I. §. 115). Auf ähnliche Weise lassen sich auch die Sätze über die Charaktere der Zahlen -1 und 2 begründen, was dem Leser überlassen bleiben mag*).

§. 52.

Nach allen diesen Untersuchungen kehren wir nun zurück zu der Beantwortung der zweiten in §. 32 aufgeworfenen Frage, welche in §. 39 auf die folgende reducirt ist:

Von welchen ungeraden Primzahlen q ist die gegebene Zahl D quadratischer Rest?

---

*) *Dirichlet* a. a. O.

Auch jetzt fragen wir nur nach denjenigen (positiv genommenen) Primzahlen q, welche nicht in D aufgehen, und setzen ausserdem der Einfachheit halber voraus, dass D durch kein Quadrat (ausser 1) theilbar ist, weil der allgemeinere Fall offenbar sogleich auf diesen einfachern reducirt werden kann. Es handelt sich also darum, allgemeine Formen anzugeben, in welchen die Primzahlen q enthalten sind, für welche das Legendre'sche Symbol $\left(\frac{D}{q}\right) = +1$ ist, und es wird sich zeigen, dass nicht blos alle diese Primzahlen q (die *Divisoren der Form* $t^2 - Du^2$ nach §. 39), sondern überhaupt alle ungeraden Zahlen Q, welche relative Primzahlen zu D sind und für welche das Jacobi'sche Symbol $\left(\frac{D}{Q}\right) = +1$ ist, in einer bestimmten Anzahl von Linearformen, d. h. von arithmetischen Reihen enthalten sind, deren Differenz entweder $= D$ oder $= 4D$ ist. Da wir vorausgesetzt haben, dass die positive oder negative Zahl D durch keine Quadratzahl theilbar ist, so wird, wenn wir das Product aller in D aufgehenden positiven ungeraden Primzahlen p mit P bezeichnen, entweder $D = \pm P$, oder $D = \pm 2P$ sein; falls D keine ungerade Primzahl p als Factor enthält (für welchen das Resultat aber schon in den §§. 40, 41 oder allgemeiner in §. 46, 4) und 5) angegeben ist), wird $P = 1$ zu setzen sein. Wir unterscheiden im Ganzen vier Fälle.

I. $D = \pm P \equiv 1 \pmod{4}$.

In diesem Falle ist, wenn Q irgend eine positive, ungerade Zahl bedeutet, die relative Primzahl zu D ist, zufolge des verallgemeinerten Reciprocitätssatzes

$$\left(\frac{D}{Q}\right) = \left(\frac{Q}{D}\right) = \left(\frac{Q}{P}\right);$$

es handelt sich also nur darum, alle Zahlen Q zu finden, für welche das Symbol $\left(\frac{Q}{P}\right) = +1$ ist. Lassen wir den unmittelbar evidenten Fall $D = P = 1$ unberücksichtigt, und bezeichnen wir mit $p, p', p'' \ldots$ die sämmtlichen in D aufgehenden Primzahlen, so ist

$$P = pp'p'' \ldots$$

und also

$$\left(\frac{D}{Q}\right) = \left(\frac{Q}{p}\right)\left(\frac{Q}{p'}\right)\left(\frac{Q}{p''}\right)\cdots$$

Wir denken uns nun in Bezug auf jede der Primzahlen p, p', $p''\ldots$ ein vollständiges Restsystem (immer mit Ausschluss der Zahlen, welche $\equiv 0$ sind) aufgeschrieben; bezeichnet man mit k, k', $k''\ldots$ beliebige, aus diesen Restsystemen in Bezug auf die Moduln p, p', $p''\ldots$ herausgegriffene, Individuen, so wird durch die Congruenzen

$$m \equiv k \text{ (mod. } p), \quad m \equiv k' \text{ (mod. } p'), \quad m \equiv k'' \text{ (mod. } p'') \ldots$$

(nach §. 25) eine und nur eine Zahlclasse m in Bezug auf den Modul $P = p\,p'\,p''\ldots$ bestimmt, welche immer nur relative Primzahlen gegen P enthält; und da k, k', $k''\ldots$ resp. $p-1$, $p'-1$, $p''-1\ldots$ verschiedene Werthe annehmen können, so erhält man im Ganzen

$$(p-1)(p'-1)(p''-1)\cdots = \varphi(P)$$

verschiedene solche Systeme von Congruenzen, durch welche die sämmtlichen $\varphi(P)$ Zahlclassen nach dem Modul P bestimmt werden, die relative Primzahlen zu P enthalten. Je nachdem nun eine gerade oder ungerade Anzahl der Symbole

$$\left(\frac{k}{p}\right),\ \left(\frac{k'}{p'}\right),\ \left(\frac{k''}{p''}\right)\cdots$$

den Werth -1 hat, wird $\left(\frac{m}{P}\right) = +1$ oder $= -1$. Es leuchtet aber ein, dass beide Fälle gleich oft vorkommen werden; für den Fall nämlich, dass nur eine einzige Primzahl p in D aufgeht, ist dies unmittelbar evident, weil unter den Zahlen k gleich viele Reste und Nichtreste von p sind; und wenn D noch andere Primzahlen p', $p''\ldots$ enthält, so wird für jedes der $(p'-1)(p''-1)\ldots$ möglichen Systeme von Werthen, welche den Zahlen k', $k''\ldots$ beigelegt sind, das Product

$$\left(\frac{k'}{p'}\right)\left(\frac{k''}{p''}\right)\cdots$$

ein bestimmtes Zeichen haben, und giebt man nun dem k alle seine $p-1$ Werthe, von denen die eine Hälfte die quadratischen Reste, die andere die quadratischen Nichtreste von p enthält, so wird das Product

$$\left(\frac{k}{p}\right)\left(\frac{k'}{p'}\right)\left(\frac{k''}{p''}\right)\cdots$$

ebenso oft, nämlich $\frac{1}{2}(p-1)$ mal, den Werth $+1$ wie den Werth -1 erhalten, und wiederholt man dasselbe mit allen $(p'-1)$ $(p''-1)$ . . möglichen Combinationen von $k', k'' \ldots$, so wird das Product

$$\left(\frac{k}{p}\right)\left(\frac{k'}{p'}\right)\left(\frac{k''}{p''}\right)\cdots=\left(\frac{m}{P}\right)$$

ebenso oft, nämlich $\frac{1}{2}\varphi(P)$ mal, den Werth $+1$, wie den Werth -1 annehmen. Die sämmtlichen $\varphi(P)$ Zahlen, welche $< P$ und relative Primzahlen zu P sind (wo P irgend eine ungerade durch kein Quadrat theilbare Zahl > 1 bedeutet), zerfallen daher in zwei Gruppen; die eine Gruppe enthält die $\frac{1}{2}\varphi(P)$ Zahlen a, für welche $\left(\frac{a}{P}\right)=1$, die andere die $\frac{1}{2}\varphi(P)$ Zahlen b, für welche $\left(\frac{b}{P}\right)=-1$ ist. Dieser Satz lässt sich auch so fassen, dass für jede solche Zahl P stets

$$\Sigma\left(\frac{m}{P}\right)=0$$

ist, wo der Buchstabe m alle Zahlen durchlaufen muss, die relative Primzahlen zu P und $< P$ sind (vergl. Supplemente I. §. 116).

Aus dieser Betrachtung folgt nun, dass alle die gesuchten (positiven ungeraden) Zahlen Q, für welche $\left(\frac{D}{Q}\right)=+1$ ist, in einer der $\frac{1}{2}\varphi(P)$ Linearformen

$$Px+a$$

und alle diejenigen, für welche $\left(\frac{D}{Q}\right)=-1$ ist, in einer der $\frac{1}{2}\varphi(P)$ Linearformen

$$Px+b$$

enthalten sind, wo x eine unbestimmte ganze Zahl bedeutet.

Wie nun in jedem gegebenen Fall die Zahlen a und b am einfachsten gefunden werden, wird man am besten aus einem Beispiel ersehen. Es sei $D=21$, also auch $P=21=3\cdot 7$; dann giebt es 12 Zahlen m, welche in der folgenden Tabelle die erste Horizontalreihe einnehmen,

m	1	2	4	5	8	10	11	13	16	17	19	20
$\left(\frac{m}{3}\right)$	+	—	+	—	—	+	—	+	+	—	+	—
$\left(\frac{m}{7}\right)$	+	+	+	—	+	—	+	—	+	—	—	—
$\left(\frac{m}{21}\right)$	+	—	+	+	—	—	—	—	+	+	—	+

in der zweiten Horizontalreihe sind die Vorzeichen von $\left(\frac{m}{3}\right)$, in der dritten die von $\left(\frac{m}{7}\right)$ angegeben; hieraus ergiebt sich durch Multiplication die vierte Horizontalreihe, in welcher sich die Vorzeichen von $\left(\frac{m}{21}\right)$ finden. Die Zahlen a sind daher

$$1,\ 4,\ 5,\ 16,\ 17,\ 20$$

und die Zahlen b folgende

$$2,\ 8,\ 10,\ 11,\ 13,\ 19.$$

Man sieht aber sofort ein, dass man diese Arbeit nur zur Hälfte, nämlich nur für die Zahlen m' auszuführen braucht, welche $< \frac{1}{2} P$ sind; denn für die übrigen Zahlen $m = P - m'$ ist

$$\left(\frac{m}{P}\right) = \left(\frac{-m'}{P}\right) = (-1)^{\frac{1}{2}(P-1)} \cdot \left(\frac{m'}{P}\right).$$

Endlich kann man auch, ohne auf die Zerlegung der Zahl P in ihre Primfactoren zurückzugehen, für jede einzelne der Zahlen m' den Werth $\left(\frac{m'}{P}\right)$ nach §. 47 mit Hülfe des allgemeinen Reciprocitätssatzes bestimmen.

In unserm Beispiel ergiebt sich daher, dass alle (positiven ungeraden) Zahlen Q, für welche $\left(\frac{21}{Q}\right) = 1$ ist, in den sechs Reihen

$$21x + 1,\ 4,\ 5,\ 16,\ 17,\ 20,$$

und dass alle solche Zahlen Q, für welche $\left(\frac{21}{Q}\right) = -1$ ist, in den sechs Reihen

$$21x + 2, \ 8, \ 10, \ 11, \ 13, \ 19$$

enthalten sind.

II. $D = \pm P \equiv 3 \pmod{4}$.

In diesem Falle wird, wenn Q wieder irgend eine positive ungerade Zahl bedeutet, welche mit D keinen gemeinschaftlichen Divisor hat,

$$\left(\frac{D}{Q}\right) = (-1)^{\frac{1}{2}(Q-1)}\left(\frac{Q}{D}\right) = (-1)^{\frac{1}{2}(Q-1)}\left(\frac{Q}{P}\right)$$

woraus sich ergiebt, dass bei der Eintheilung sämmtlicher Zahlen Q in zwei Classen nicht bloss ihr Verhalten zum Modul P, sondern auch zum Modul 4 in Betracht zu ziehen ist. Behalten wir dieselbe Bezeichnungsweise wie im ersten Fall bei, so wird $\left(\frac{D}{Q}\right) = +1$ sein, so oft

$$Q \equiv 1 \pmod{4} \quad \text{und} \quad Q \equiv a \pmod{P}$$

oder

$$Q \equiv 3 \pmod{4} \quad \text{und} \quad Q \equiv b \pmod{P};$$

und es wird $\left(\frac{D}{Q}\right) = -1$ sein, so oft

$$Q \equiv 1 \pmod{4} \quad \text{und} \quad Q \equiv b \pmod{P}$$

oder

$$Q \equiv 3 \pmod{4} \quad \text{und} \quad Q \equiv a \pmod{P}.$$

Nun wird (nach §. 25) jedem dieser vier Congruenzpaare eine und nur eine Classe von Zahlen nach dem Modul $4P$ entsprechen, welche relative Primzahlen zu $4P$ sind; und da die Anzahl sowohl der Zahlen a als auch der Zahlen b gleich $\frac{1}{2}\varphi(P)$ ist, so werden sämmtliche Zahlen Q, für welche $\left(\frac{D}{Q}\right) = +1$ ist, in $\varphi(P) = \frac{1}{2}\varphi(4P)$ arithmetischen Reihen von der Form

$$4Px + \alpha,$$

und ebenso werden alle Zahlen Q, für welche $\left(\frac{D}{Q}\right) = -1$ ist, in ebensoviel arithmetischen Reihen von der Form

$$4Px + \beta$$

enthalten sein; die Zahlen α und β erschöpfen zusammen alle $\varphi(4P)$ Zahlen, die kleiner als $4P$ und relative Primzahlen zu $4P$ sind.

Ist z. B. $D = +P = 15$, so sind die relativen Primzahlen zu 60 zu betrachten:

$$\begin{array}{l} 1,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29; \\ 59,\ 53,\ 49,\ 47,\ 43,\ 41,\ 37,\ 31; \end{array}$$

diese zerfallen in die Zahlen α, nämlich

$$\begin{array}{l} 1,\ 7,\ 11,\ 17, \\ 59,\ 53,\ 49,\ 43, \end{array}$$

und in die Zahlen β, nämlich

$$\begin{array}{l} 13,\ 19,\ 23,\ 29, \\ 47,\ 41,\ 37,\ 31. \end{array}$$

III. $D = \pm 2P \equiv 2 \pmod{8}$.

In diesem Falle ist $\pm P \equiv 1 \pmod{4}$ und folglich

$$\left(\frac{D}{Q}\right) = \left(\frac{2}{Q}\right)\left(\frac{\pm P}{Q}\right) = (-1)^{1/8(Q^2-1)}\left(\frac{Q}{P}\right);$$

ausser der Relation von Q zum Modul P ist daher auch noch die Relation von Q zum Modul 8 zu betrachten. Es wird $\left(\frac{D}{Q}\right) = +1$ sein, wenn

$$Q \equiv 1 \pmod{8} \quad \text{und} \quad Q \equiv a \pmod{P}$$

oder

$$Q \equiv 3 \pmod{8} \quad \text{und} \quad Q \equiv b \pmod{P}$$

oder

$$Q \equiv 5 \pmod{8} \quad \text{und} \quad Q \equiv b \pmod{P}$$

oder

$$Q \equiv 7 \pmod{8} \quad \text{und} \quad Q \equiv a \pmod{P};$$

hieraus ergiebt sich (nach §. 25) ähnlich wie in dem vorigen Fall, dass diese Zahlen Q in $2\varphi(P) = \frac{1}{2}\varphi(8P)$ arithmetischen Reihen von der Form

$$8Px + \alpha'$$

enthalten sind, während aus den vier andern Fällen

$$Q \equiv 1 \pmod{8} \quad \text{und} \quad Q \equiv b \pmod{P}$$

oder

$$Q \equiv 3 \pmod{8} \quad \text{und} \quad Q \equiv a \pmod{P}$$

oder

$$Q \equiv 5 \pmod{8} \quad \text{und} \quad Q \equiv a \pmod{P}$$

oder

$$Q \equiv 7 \pmod{8} \quad \text{und} \quad Q \equiv b \pmod{P}$$

wieder $\frac{1}{2}\varphi(8P)$ arithmetische Reihen von der Form

$$8Px + \beta'$$

entspringen, in welchen alle Zahlen Q enthalten sind, für welche $\left(\frac{D}{Q}\right) = -1$ ist.

Ist z. B. $D = -6$, also $P = 3$, so sind die relativen Primzahlen zu 24 zu betrachten, und man findet leicht wie früher, dass die Zahlen α' folgende

$$1, \ 5, \ 7, \ 11$$

und die Zahlen β' folgende

$$23, \ 19, \ 17, \ 13$$

sind.

IV. $D = \pm 2P \equiv 6 \pmod{8}$.

In diesem Fall ist $\pm P \equiv 3 \pmod{4}$ und folglich

$$\left(\frac{D}{Q}\right) = \left(\frac{-2}{Q}\right)\left(\frac{\mp P}{Q}\right) = (-1)^{\frac{1}{8}(Q^2-1) + \frac{1}{2}(Q-1)} \left(\frac{Q}{P}\right);$$

aus den vier Fällen

$$Q \equiv 1 \pmod{8} \quad \text{und} \quad Q \equiv a \pmod{P}$$
$$Q \equiv 3 \pmod{8} \quad \text{und} \quad Q \equiv a \pmod{P}$$
$$Q \equiv 5 \pmod{8} \quad \text{und} \quad Q \equiv b \pmod{P}$$
$$Q \equiv 7 \pmod{8} \quad \text{und} \quad Q \equiv b \pmod{P}$$

entspringen $\frac{1}{2}\varphi(8P)$ arithmetische Reihen von der Form

$$8Px + \alpha'',$$

welche alle Zahlen Q enthalten, für welche $\left(\frac{D}{Q}\right) = +1$ ist; und

ebenso sind alle Zahlen Q, für welche $\left(\frac{D}{Q}\right) = -1$, in eben so vielen arithmetischen Reihen von der Form

$$8Px + \beta''$$

enthalten, welche den vier Fällen

$$Q \equiv 1 \text{ (mod. 8) und } Q \equiv b \text{ (mod. } P)$$
$$Q \equiv 3 \text{ (mod. 8) und } Q \equiv b \text{ (mod. } P)$$
$$Q \equiv 5 \text{ (mod. 8) und } Q \equiv a \text{ (mod. } P)$$
$$Q \equiv 7 \text{ (mod. 8) und } Q \equiv a \text{ (mod. } P)$$

entsprechen.

Ist z. B. $D = 6$, also $P = 3$, so sind

$$1, \ 5, \ 19, \ 23$$

die Zahlen α'', und

$$7, \ 11, \ 13, \ 17$$

die Zahlen β''.

Vierter Abschnitt.

Von den quadratischen Formen.

§. 53.

Unter einer *Form* versteht man in der Zahlentheorie im Allgemeinen eine ganze rationale Function von Variabeln, deren Coefficienten ganze Zahlen sind (vergl. §. 39). Je nach dem Grade derselben unterscheidet man lineare, quadratische, cubische Formen u. s. w.; je nach der Anzahl der vorkommenden Variabeln spricht man von binären, ternären Formen u. s. w. Wir werden uns im Folgenden ausschliesslich mit Ausdrücken von der Form

$$ax^2 + 2bxy + cy^2$$

beschäftigen, wo a, b, c bestimmte, gegebene ganze Zahlen, x und y aber unbestimmte, variabele ganze Zahlen bedeuten; und wir werden diese homogenen binären quadratischen Formen, wo kein Missverständniss zu besorgen ist, kurz Formen nennen.

Wir haben dem Coefficienten des Productes xy der beiden Variabeln gleich die Gestalt einer geraden Zahl $2b$ gegeben, weil die Untersuchung dadurch erleichtert wird; sollte in einer Form dieser Coefficient eine ungerade Zahl sein, so würde es genügen, die ganze Form mit 2 zu multipliciren, um diesen Fall auf den obigen zurückzuführen, und aus den Eigenschaften der so erhaltenen Form würde man mit Leichtigkeit auf die Eigenschaften der ursprünglichen Form zurückschliessen können.

Sind die drei Glieder in der obigen Anordnung geschrieben, so nennt man a den *ersten*, b (nicht $2b$) den *zweiten*, c den *dritten Coefficienten;* a und c fasst man wohl auch unter dem gemeinschaftlichen Namen der *äussern* Coefficienten zusammen, und nennt dann b im Gegensatz den *mittlern* Coefficienten; ähnlich heisst x die *erste*, y die *zweite Variabele.* Eine solche Form bezeichnet man wohl auch kurz durch das Symbol (a, b, c), wenn es sich nur darum handelt, die Coefficienten anzugeben, von denen allein die Eigenschaften der Form abhängen können.

Wir schliessen nun ein für alle Mal die Fälle aus, in welchen die Form sich in zwei lineare Factoren mit *rationalen* Coefficienten zerfällen lässt, weil diese eine andere und zwar einfachere Behandlung gestatten. Zunächst folgt hieraus, dass in den Formen, mit welchen allein wir uns beschäftigen wollen, keiner der äussern Coefficienten gleich Null sein wird; da ferner

$$ax^2 + 2bxy + cy^2 = \frac{1}{a}\left((ax + by)^2 - (b^2 - ac)\, y^2\right)$$

ist, so ergiebt sich weiter, dass die Zahl $b^2 - ac$ nie eine vollständige Quadratzahl sein darf, denn sonst würde die Form

$$ax^2 + 2bxy + cy^2 =$$
$$\frac{1}{a}\left(ax + (b + \sqrt{b^2 - ac})\, y\right)\left(ax + (b - \sqrt{b^2 - ac})\, y\right)$$

ein Product aus zwei linearen Factoren mit rationalen Coefficienten sein. Die Zahl $b^2 - ac$, von welcher, wie wir sehen werden, die Eigenschaften der Form (a, b, c) hauptsächlich abhängen, heisst die *Determinante* dieser Form; wir werden sie im Folgenden mit dem Buchstaben D bezeichnen. Die unsern Formen (a, b, c) auferlegte Beschränkung besteht also darin, dass $\sqrt{D}$ stets irrational ist.

Euler hat sich zuerst mit solchen Formen, aber nur von specieller Natur, beschäftigt; erst *Lagrange* legte den Grund zu einer allgemeinen Theorie derselben, die dann später von *Legendre*, vor Allen aber durch *Gauss* bedeutend vervollständigt wurde.

Ihre Entstehung verdankt die ganze Theorie dem Probleme, zu entscheiden, ob eine gegebene Zahl m durch die gegebene Form (a, b, c) *darstellbar* ist, d. h. ob es specielle Werthe von x, y giebt, für welche die Form den Werth m erhält. Doch ist zur

vollständigen Lösung desselben die Theorie der *Transformation* erforderlich, mit welcher wir uns daher zunächst beschäftigen wollen.

§. 54.

Ebenso wie die Gleichungen der Curven in der analytischen Geometrie ihre Gestalt ändern, wenn ein anderes Coordinatensystem gewählt wird, so geht eine quadratische Form (a, b, c) durch Einführung zweier neuen Variabeln in eine neue quadratische Form (a', b', c') über. Sind nämlich x, y die Variabeln der Form (a, b, c), und setzt man

$$\begin{aligned} x &= \alpha x' + \beta y', \\ y &= \gamma x' + \delta y', \end{aligned} \tag{1}$$

wo $\alpha, \beta, \gamma, \delta$ vier bestimmte ganze Zahlen, und x', y' die neuen Variabeln bedeuten, so wird

$$ax^2 + 2bxy + cy^2 = a'x'^2 + 2b'x'y' + c'y'^2,$$

und die Coefficienten a', b', c' der neuen quadratischen Form hängen auf folgende Weise von denen der ursprünglichen Form und von den vier Coefficienten $\alpha, \beta, \gamma, \delta$ ab:

$$\begin{aligned} a' &= a\alpha^2 + 2b\alpha\gamma + c\gamma^2 \\ b' &= a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta \\ c' &= a\beta^2 + 2b\beta\delta + c\delta^2. \end{aligned} \tag{2}$$

Man drückt den Zusammenhang der beiden Formen kurz so aus: die Form $ax^2 + 2bxy + cy^2$ geht durch die *Transformation* oder *Substitution* (1) in die Form $a'x'^2 + 2b'x'y' + c'y'^2$ über. Die Zahlen $\alpha, \beta, \gamma, \delta$ heissen der Reihe nach der *erste*, *zweite*, *dritte*, *vierte Coefficient* der Substitution. Da die Wahl der Buchstaben zur Bezeichnung der Variabeln von ganz untergeordneter Bedeutung ist, und die Natur der Formen nur von den Coefficienten abhängt, so drückt man sich häufig noch kürzer so aus: die Form (a, b, c) geht durch die Substitution $\begin{pmatrix}\alpha, & \beta \\ \gamma, & \delta\end{pmatrix}$ in die Form (a', b', c') über; und es ist offenbar, dass diese Ausdrucksweise nicht mehr oder weniger sagt, als dass die drei Gleichungen (2) Statt finden. Hierbei ist wohl auf die Stellung der Coefficienten der Formen sowohl, wie derjenigen der Substitution zu achten;

behalten wir die eben eingeführten Bezeichnungen bei, so müssen wir z. B. sagen, dass gleichzeitig die Form (a, b, c) durch die Substitution $\begin{pmatrix}\beta, & \alpha\\ \delta, & \gamma\end{pmatrix}$ in die Form (c', b', a'), ferner dass die Form (c, b, a) durch die Substitution $\begin{pmatrix}\gamma, & \delta\\ \alpha, & \beta\end{pmatrix}$ in die Form (a', b', c'), und endlich dass die Form (c, b, a) durch die Substitution $\begin{pmatrix}\delta, & \gamma\\ \beta, & \alpha\end{pmatrix}$ in die Form (c', b', a') übergeht.

Es leuchtet ein, dass jede durch die zweite Form (a', b', c') darstellbare Zahl auch durch die erste Form (a, b, c) dargestellt werden kann; denn wird die Zahl m durch (a', b', c') dargestellt, indem den Variabeln x', y' die speciellen Werthe r', s' ertheilt werden, so setze man

$$r = \alpha r' + \beta s', \quad s = \gamma r' + \delta s',$$

und es wird die Form (a, b, c) dieselbe Zahl m darstellen, sobald $x = r$, $y = s$ gesetzt wird. Man sagt deshalb auch: die Form (a, b, c) *enthält* die Form (a', b', c'), oder deutlicher: die Form (a', b', c') ist unter der Form (a, b, c) *enthalten*; eben weil sämmtliche durch (a', b', c') darstellbare Zahlen unter den durch (a, b, c) darstellbaren enthalten sind *).

Von besonderer Wichtigkeit ist die Relation, in welcher die Determinante

$$D' = b'^2 - a'c'$$

der neuen Form zu der der früheren steht; substituirt man für a', b', c' ihre Ausdrücke gemäss den Gleichungen (2), so findet man nach leichten Reductionen

$$D' = (\alpha\delta - \beta\gamma)^2 D;$$

die neue Determinante ist daher stets gleich der alten, multiplicirt mit einer Quadratzahl; beide Determinanten haben also auch dasselbe Vorzeichen. Da wir von vorn herein Formen ausschliessen, deren Determinanten $= 0$ sind, so betrachten wir deshalb auch nur solche Substitutionen $\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}$, für welche die Coefficientenverbindung $\alpha\delta - \beta\gamma$ einen von Null verschiedenen Werth hat. Hieran knüpft sich jedoch noch eine wichtige Unterscheidung;

*) Ueber die Umkehrung dieses Satzes siehe eine Abhandlung von *Schering* in Liouville's Journal 1859.

je nachdem nämlich dieser Ausdruck $\alpha\delta - \beta\gamma$ einen positiven oder negativen Werth hat, soll die Substitution $\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}$ eine *eigentliche* oder *uneigentliche* heissen, und diese Ausdrucksweise soll auf die Beziehung zwischen den Formen (a, b, c) und (a', b', c') übertragen werden, indem wir sagen, dass die Form (a', b', c') *eigentlich* oder *uneigentlich* unter der Form (a, b, c) *enthalten* sei, je nachdem die Substitution $\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}$, durch welche die letztere in die erstere übergeht, eigentlich oder uneigentlich ist. Um Missverständnisse zu vermeiden, fügen wir sogleich hinzu, dass eine Form eine andere sowohl eigentlich als auch uneigentlich enthalten kann; denn es tritt häufig der Fall ein, dass eine Form einmal durch eine eigentliche, ein anderes Mal durch eine uneigentliche Substitution in eine und dieselbe zweite Form transformirt wird. So z. B. geht die Form $(3, 13, 18)$ durch die eigentliche Substitution $\begin{pmatrix}+1, & 0\\ -1, & +1\end{pmatrix}$, und ebenso durch die uneigentliche Substitution $\begin{pmatrix}+1, & +2\\ -1, & -3\end{pmatrix}$ in die andere Form $(-5, -5, 18)$ über; die erstere enthält daher die letztere sowohl eigentlich als auch uneigentlich.

§. 55.

Behalten wir die vorhergehenden Bezeichnungen bei, und nehmen wir an, dass die Form

$$(a', b', c') = a'x'^2 + 2b'x'y' + c'y'^2$$

durch eine neue Substitution

$$x' = \alpha'x'' + \beta'y''$$
$$y' = \gamma'x'' + \delta'y''$$

in die Form

$$(a'', b'', c'') = a''x''^2 + 2b''x''y'' + c''y''^2$$

übergeht, so geht offenbar die erste Form (a, b, c) durch die Substitution

$$x = \alpha(\alpha'x'' + \beta'y'') + \beta(\gamma'x'' + \delta'y'')$$
$$y = \gamma(\alpha'x'' + \beta'y'') + \delta(\gamma'x'' + \delta'y'')$$

oder

$$x = (\alpha\alpha' + \beta\gamma')\, x'' + (\alpha\beta' + \beta\delta')\, y''$$
$$y = (\gamma\alpha' + \delta\gamma')\, x'' + (\gamma\beta' + \delta\delta')\, y''$$

in die dritte Form (a'', b'', c'') über. Hieraus folgt der Satz:

Enthält eine Form eine zweite, diese wieder eine dritte, so enthält auch die erste Form die dritte.

Bezeichnet man nun die Coefficientenverbindung

$$(\alpha\alpha' + \beta\gamma')(\gamma\beta' + \delta\delta') - (\alpha\beta' + \beta\delta')(\gamma\alpha' + \delta\gamma')$$

mit ε, so ist nothwendig die Determinante der dritten Form $D'' = \varepsilon^2 D$; da aber andererseits

$$D' = (\alpha\delta - \beta\gamma)^2 D,\quad D'' = (\alpha'\delta' - \beta'\gamma')^2 D',$$

also auch

$$D'' = (\alpha\delta - \beta\gamma)^2 (\alpha'\delta' - \beta'\gamma')^2 D,$$

und D von Null verschieden ist, so schliessen wir hieraus, dass

$$\varepsilon^2 = (\alpha\delta - \beta\gamma)^2 (\alpha'\delta' - \beta'\gamma')^2$$

ist, und man überzeugt sich leicht durch Vergleichung beider Seiten, dass die Quadratwurzel in folgender Weise auszuziehen ist:

$$\varepsilon = (\alpha\delta - \beta\gamma)(\alpha'\delta' - \beta'\gamma').$$

Aus dieser Gleichung (welche einen der einfachsten Sätze der Determinantentheorie enthält) folgt noch eine wesentliche Vervollständigung des obigen Satzes, nämlich:

Die erste Form enthält die dritte eigentlich oder uneigentlich, je nachdem die Arten, in welcher die erste die zweite, die zweite die dritte enthält, gleichartig oder ungleichartig sind.

Fährt man in derselben Weise fort und transformirt die dritte Form in eine vierte, diese in eine fünfte u. s. f., so ergiebt sich unmittelbar der allgemeine Satz: Wenn von einer Reihe von Formen jede die nächstfolgende enthält, so enthält die erste Form auch die letzte, und zwar eigentlich oder uneigentlich, je nachdem es eine gerade oder ungerade Anzahl von Malen vorkommt, dass eine Form die nächstfolgende uneigentlich enthält.

Die Substitution, durch welche die erste Form unmittelbar in die letzte transformirt wird, heisst *zusammengesetzt* aus den einzelnen successiven Substitutionen; um die Zusammensetzung von zwei Substitutionen anzudeuten, wollen wir uns bisweilen der Bezeichnung

$$\begin{pmatrix}\alpha, \beta\\ \gamma, \delta\end{pmatrix}\begin{pmatrix}\alpha', \beta'\\ \gamma', \delta'\end{pmatrix} = \begin{pmatrix}\alpha\alpha' + \beta\gamma', & \alpha\beta' + \beta\delta'\\ \gamma\alpha' + \delta\gamma', & \gamma\beta' + \delta\delta'\end{pmatrix}$$

bedienen; offenbar ist es im Allgemeinen nicht erlaubt, die Ordnung der beiden successiven Substitutionen umzukehren, weil hierdurch auch die resultirende Substitution geändert würde. So ist z. B.

$$\begin{pmatrix}+1, 0\\ -1, 1\end{pmatrix}\begin{pmatrix}+1, +2\\ -1, -3\end{pmatrix} = \begin{pmatrix}+1, +2\\ -2, -5\end{pmatrix}$$

$$\begin{pmatrix}+1, +2\\ -1, -3\end{pmatrix}\begin{pmatrix}+1, 0\\ -1, 1\end{pmatrix} = \begin{pmatrix}-1, +2\\ +2, -3\end{pmatrix}.$$

Dagegen ist es bei drei successiven Substitutionen S, S', S'' gleichgültig, ob man erst S und S' zusammensetzt, und dann das Resultat SS' mit S'' verbindet, oder ob man S mit dem Resultat $S'S''$ der zweiten und dritten Substitution zusammensetzt; in Zeichen:

$$(SS')S'' = S(S'S'').$$

Dies folgt unmittelbar aus dem Begriffe dieser Zusammensetzung; denn sind (x, y), (x', y'), (x'', y'') und (x''', y''') die successiven Variabeln, so ist es für die Ausdrücke von x, y durch x''', y''' gleichgültig, ob man die Variabeln x'', y'' oder die Variabeln x', y' als Zwischenglieder einschiebt.

Ferner ist für die Folge zu bemerken, dass die Substitution $\begin{pmatrix}1, 0\\ 0, 1\end{pmatrix}$ bei der Zusammensetzung stets fortgelassen werden darf, da sie keine Aenderung hervorbringt.

§ 56.

Besonders wichtig ist nun die Frage: wann enthalten zwei Formen sich gegenseitig? Offenbar ist dann das System aller durch die eine Form darstellbaren Zahlen identisch mit dem System derjenigen Zahlen, welche durch die andere Form dargestellt werden können. Zwei solche Formen werden wir *äquivalent* nennen. Sind D, D' ihre Determinanten, so muss sowohl $\frac{D'}{D}$, als auch $\frac{D}{D'}$, eine ganze Quadratzahl, also eine ganze positive

Zahl sein, und hieraus folgt als eine für die Aequivalenz zweier Formen *erforderliche* Bedingung, dass ihre Determinanten D und D' gleich sein müssen.

Diese Bedingung ist aber umgekehrt *nicht hinreichend*, um auf die Aequivalenz schliessen zu können. Dies ist erst dann gestattet, wenn man ausserdem weiss, dass die eine der beiden Formen die andere enthält. In der That, wenn die beiden Formen (a, b, c) und (a', b', c') gleiche Determinanten haben, und wenn ausserdem die erstere durch die Substitution

$$x = \alpha x' + \beta y'$$
$$y = \gamma x' + \delta y'$$

in die letztere übergeht, so folgt aus der Relation

$$D' = (\alpha\delta - \beta\gamma)^2 D$$

und der Gleichheit von D' und D die Gleichung

$$\alpha\delta - \beta\gamma = \pm 1$$

und hieraus, wenn man zur Abkürzung $\alpha\delta - \beta\gamma = \pm 1 = \varepsilon$ setzt,

$$x' = + \varepsilon\delta x - \varepsilon\beta y$$
$$y' = - \varepsilon\gamma x + \varepsilon\alpha y$$

und es geht daher durch diese Substitution mit ganzzahligen Coefficienten die Form (a', b', c') in die Form (a, b, c) über; also sind in der That beide Formen einander äquivalent. Die Substitutionen

$$\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix} \quad \text{und} \quad \begin{pmatrix} + \varepsilon\delta, & - \varepsilon\beta \\ - \varepsilon\gamma, & + \varepsilon\alpha \end{pmatrix},$$

deren jede die *inverse* der andern heisst, und durch deren Zusammensetzung immer die Substitution $\begin{pmatrix} 1, & 0 \\ 0, & 1 \end{pmatrix}$ entsteht, sind offenbar entweder beide eigentlich, oder beide uneigentlich; je nachdem das Eine oder das Andere Statt findet, sollen die beiden Formen *eigentlich* oder *uneigentlich äquivalent* heissen.

Sowie wir eben gesehen haben, dass die eine von zwei äquivalenten Formen in die andere immer durch eine Substitution $\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}$ übergeht, in welcher $\alpha\delta - \beta\gamma = \pm 1$ ist, so leuchtet auch umgekehrt ein, dass durch jede solche Substitution eine beliebige

Form nothwendig in eine ihr äquivalente transformirt wird; denn die Determinanten beider Formen sind einander gleich. Hierin besteht also die *erforderliche und hinreichende* Bedingung für die Aequivalenz zweier Formen.

Aus dem Begriffe der Aequivalenz ergiebt sich unmittelbar, dass jede Form sich selbst eigentlich äquivalent ist; denn sie geht durch die eigentliche Substitution $\begin{pmatrix}1, & 0\\ 0, & 1\end{pmatrix}$ in sich selbst über. Ferner folgt unmittelbar aus dem oben angeführten Satz über die Transformation in Bezug auf eine Reihe von Formen folgender analoge Satz über die Aequivalenz:

Wenn in einer Reihe von Formen jede der nächstfolgenden äquivalent ist, so ist die erste auch der letzten äquivalent, und zwar eigentlich oder uneigentlich, je nachdem die uneigentliche Aequivalenz zweier successiver Formen in dieser Kette eine gerade oder ungerade Anzahl von Malen vorkommt.

§. 57.

Auch hier bei der Aequivalenz schliesst die eine Art derselben die andere nicht aus; es kommt häufig der Fall vor, dass zwei Formen einander sowohl eigentlich als uneigentlich äquivalent sind; in dem weiter oben angeführten Beispiel sind wirklich die beiden Formen (3, 13, 18) und (— 5, — 5, 18) eigentlich und uneigentlich äquivalent; die erstere geht durch die Substitutionen

$$\begin{pmatrix}+1, & 0\\ -1, & 1\end{pmatrix} \quad \text{und} \quad \begin{pmatrix}+1, & +2\\ -1, & -3\end{pmatrix}$$

in die letztere über, und umgekehrt diese in jene durch die inversen Substitutionen

$$\begin{pmatrix}1, & 0\\ 1, & 1\end{pmatrix} \quad \text{und} \quad \begin{pmatrix}+3, & +2\\ -1, & -1\end{pmatrix}.$$

Wenn zwei Formen sowohl eigentlich als uneigentlich äquivalent sind, so ist jede von ihnen sich selbst uneigentlich äquivalent.

Denn, wenn die Form (a, b, c) durch jede der beiden Substitutionen

$$\begin{pmatrix}\alpha', & \beta'\\ \gamma', & \delta'\end{pmatrix} \quad \text{und} \quad \begin{pmatrix}\alpha'', & \beta''\\ \gamma'', & \delta''\end{pmatrix},$$

in denen

$$\alpha'\delta' - \beta'\gamma' = +1, \quad \alpha''\delta'' - \beta''\gamma'' = -1,$$

in die Form (a', b', c') übergeht, so geht (a', b', c') durch jede der beiden inversen Substitutionen

$$\begin{pmatrix} +\delta', & -\beta' \\ -\gamma', & +\alpha' \end{pmatrix} \text{ und } \begin{pmatrix} -\delta'', & +\beta'' \\ +\gamma'', & -\alpha'' \end{pmatrix}$$

in (a, b, c) über; und hieraus folgt, dass (a, b, c) durch jede der beiden zusammengesetzten, und zwar nothwendig uneigentlichen Substitutionen

$$\begin{pmatrix} \alpha', & \beta' \\ \gamma', & \delta' \end{pmatrix}\begin{pmatrix} -\delta'', & +\beta'' \\ +\gamma'', & -\alpha'' \end{pmatrix} \text{ und } \begin{pmatrix} \alpha'', & \beta'' \\ \gamma'', & \delta'' \end{pmatrix}\begin{pmatrix} +\delta', & -\beta' \\ -\gamma', & +\alpha' \end{pmatrix}$$

in sich selbst übergeht. So z. B. geht die Form (3, 13, 18) durch die uneigentlichen Substitutionen

$$\begin{pmatrix} +1, & 0 \\ -1, & 1 \end{pmatrix}\begin{pmatrix} +3, & +2 \\ -1, & -1 \end{pmatrix} = \begin{pmatrix} +3, & +2 \\ -4, & -3 \end{pmatrix}$$

und

$$\begin{pmatrix} +1, & +2 \\ -1, & -3 \end{pmatrix}\begin{pmatrix} 1, & 0 \\ 1, & 1 \end{pmatrix} = \begin{pmatrix} +3, & +2 \\ -4, & -3 \end{pmatrix}$$

in sich selbst über.

Es ist kein Zufall, dass diese beiden auf verschiedene Art zusammengesetzten Substitutionen identisch ausfallen; setzt man nämlich

$$\begin{pmatrix} \alpha', & \beta' \\ \gamma', & \delta' \end{pmatrix}\begin{pmatrix} -\delta'', & +\beta'' \\ +\gamma'', & -\alpha'' \end{pmatrix} = \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix},$$

so findet man zunächst

$$\begin{pmatrix} \alpha'', & \beta'' \\ \gamma'', & \delta'' \end{pmatrix}\begin{pmatrix} +\delta', & -\beta' \\ -\gamma', & +\alpha' \end{pmatrix} = \begin{pmatrix} -\delta, & +\beta \\ +\gamma, & -\alpha \end{pmatrix},$$

und wir haben daher, um die Identität dieser beiden Substitutionen nachzuweisen, nur noch zu zeigen, dass in jeder uneigentlichen Substitution $\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}$, durch welche eine Form in sich selbst übergeht, stets der erste und vierte Coefficient einander gleich, aber entgegengesetzt sind. Dies geschieht leicht auf folgende Weise. Wenn die Form (a, b, c) durch die uneigentliche Substitution $\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}$ in sich selbst übergeht, so ist

$$a\alpha^2 + (2b\alpha + c\gamma)\gamma = a$$
$$a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta = b$$
$$\alpha\delta - \beta\gamma = -1.$$

Die zweite dieser drei Gleichungen geht, wenn man der dritten gemäss $\beta\gamma$ durch $\alpha\delta + 1$ ersetzt, in folgende über:

$$a\alpha\beta + (2b\alpha + c\gamma)\delta = 0;$$

eliminirt man aus dieser und aus der ersten jener drei Gleichungen die Grösse $2b\alpha + c\gamma$, so erhält man, wenn man den Factor a wegwirft (der ja von Null verschieden ist, weil sonst die Determinante D eine Quadratzahl wäre), die Relation

$$(\alpha^2 - 1)\delta = \alpha\beta\gamma,$$

woraus mit Rücksicht auf $\alpha\delta - \beta\gamma = -1$ wirklich folgt, dass $\delta = -\alpha$ ist, was zu beweisen war.

§. 58.

Jede uneigentliche Substitution, durch welche eine Form (a, b, c) in sich selbst übergeht, ist daher nothwendig von der Form $\begin{pmatrix}\alpha, & +\beta \\ \gamma, & -\alpha\end{pmatrix}$, und es ist also gleichzeitig $\alpha^2 + \beta\gamma = 1$. Von besonderm Interesse ist der specielle Fall $\gamma = 0$; dann ist $\alpha = \pm 1$ und entsprechend $\pm a\beta = 2b$; eine solche Form, deren doppelter mittlerer Coefficient durch den ersten theilbar ist, heisst eine *forma anceps.* Und umgekehrt ist leicht zu sehen, dass jede forma anceps sich selbst uneigentlich äquivalent ist; denn wenn (a, b, c) eine solche Form, und also $2b = a\beta$ ist, so geht (a, b, c) wirklich durch die uneigentliche Substitution $\begin{pmatrix}1, & +\beta \\ 0, & -1\end{pmatrix}$ in sich selbst über. Dasselbe gilt offenbar von jeder Form, welche einer forma anceps äquivalent ist; aber es besteht auch der umgekehrte *Satz*:

Wenn eine Form sich selbst uneigentlich äquivalent ist, so giebt es stets eine ihr äquivalente forma anceps.

Beweis. Es sei φ eine solche Form, welche durch die uneigentliche Substitution $\begin{pmatrix}\alpha, & +\beta \\ \gamma, & -\alpha\end{pmatrix}$ in sich selbst übergeht; ist

$\gamma = 0$, so wissen wir, dass φ selbst eine forma anceps und folglich der Satz richtig ist. Ist aber γ von Null verschieden, so suchen wir eine eigentliche Substitution $\begin{pmatrix}\lambda, & \mu \\ \nu, & \varrho\end{pmatrix}$, durch welche die Form φ in eine ihr äquivalente forma anceps übergeht, die wir mit ψ bezeichnen wollen. Da also $\lambda\varrho - \mu\nu = +1$, und folglich ψ durch die inverse Substitution $\begin{pmatrix}+\varrho, & -\mu \\ -\nu, & +\lambda\end{pmatrix}$ in φ übergeht, so muss ψ durch die offenbar uneigentliche, aus den drei successiven Substitutionen

$$\begin{pmatrix}+\varrho, & -\mu \\ -\nu, & +\lambda\end{pmatrix}, \quad \begin{pmatrix}\alpha, & +\beta \\ \gamma, & -\alpha\end{pmatrix}, \quad \begin{pmatrix}\lambda, & \mu \\ \nu, & \varrho\end{pmatrix}$$

zusammengesetzte Substitution in sich selbst übergehen. Der dritte Coefficient dieser Substitution ist

$$\gamma\lambda^2 - 2\alpha\lambda\nu - \beta\nu^2,$$

und es kommt nur darauf an, zwei relative Primzahlen λ, ν so zu bestimmen, dass dieser Coefficient $= 0$ wird; denn dann ist ψ eine forma anceps. Diese Forderung reducirt sich, wenn man mit γ multiplicirt und bedenkt, dass $\alpha^2 + \beta\gamma = 1$ ist, auf die folgende:

$$(\gamma\lambda - \alpha\nu)^2 - \nu^2 = 0; \quad \frac{\lambda}{\nu} = \frac{\alpha \pm 1}{\gamma};$$

da unserer Annahme nach γ von Null verschieden ist, so kann man also λ und ν dieser Forderung gemäss bestimmen, und zwar als relative Primzahlen, wenn man den Bruch $\frac{\alpha \pm 1}{\gamma}$ auf seine kleinste Benennung $\frac{\lambda}{\nu}$ bringt. Dies Letztere ist erforderlich, weil ja die vier Coefficienten $\lambda, \mu, \nu, \varrho$ der Gleichung $\lambda\varrho - \mu\nu = 1$ genügen müssen. Sobald nun λ und ν auf dem angegebenen Wege bestimmt sind, so kann man dann unendlich viele Werthenpaare für ϱ und μ (nach §. 24) finden, welche diese letzte Forderung erfüllen. Auf diese Weise ist also wirklich aus $\begin{pmatrix}\alpha, & +\beta \\ \gamma, & -\alpha\end{pmatrix}$ eine eigentliche Substitution $\begin{pmatrix}\lambda, & \mu \\ \nu, & \varrho\end{pmatrix}$ gefunden, welche die gegebene Form φ in eine ihr äquivalente forma anceps ψ transformirt, und hierdurch der obige Satz bewiesen.

Nehmen wir als Beispiel die obige Form (3, 13, 18), welche durch die uneigentliche Substitution $\begin{pmatrix} +3, & +2 \\ -4, & -3 \end{pmatrix}$ in sich selbst übergeht; wir haben also nur

$$\frac{\lambda}{\nu} = \frac{3 \pm 1}{-4}$$

zu setzen; nehmen wir das obere Zeichen, so ist $\lambda = \pm 1$, $\nu = \mp 1$ zu setzen, und entsprechend $\varrho + \mu = \pm 1$. Nehmen wir die obern Zeichen und $\varrho = 1$, $\mu = 0$, so erhalten wir die Substitution $\begin{pmatrix} +1, & 0 \\ -1, & 1 \end{pmatrix}$, durch welche, wie schon oben bemerkt ist, die Form (3, 13, 18) in die Form (— 5, — 5, 18) übergeht, welche in der That eine forma anceps ist.

Ferner: Die Form (7, 1, — 1) geht durch die uneigentliche Substitution $\begin{pmatrix} +2, & +1 \\ -3, & -2 \end{pmatrix}$ in sich selbst über; in diesem Fall haben wir also

$$\frac{\lambda}{\nu} = \frac{2 \pm 1}{-3}$$

zu setzen; nehmen wir der Einfachheit halber wieder das obere Zeichen, so können wir wieder $\lambda = 1$, $\nu = -1$, $\varrho = 1$, $\mu = 0$ setzen; und in der That geht die Form (7, 1, — 1) durch die Substitution $\begin{pmatrix} +1, & 0 \\ -1, & 1 \end{pmatrix}$ in die forma anceps (4, 2, — 1) über.

§. 59.

Wir verlassen hiermit diesen interessanten Gegenstand und beschäftigen uns von jetzt an ausschliesslich mit der *eigentlichen* Aequivalenz; nur diese soll im Folgenden gemeint sein, wenn schlechthin von Aequivalenz gesprochen wird; ebenso wird unter Substitution immer nur noch die eigentliche Substitution verstanden werden. Die beiden Hauptprobleme in der Theorie der Aequivalenz sind die folgenden:

I. *Zu entscheiden, ob zwei gegebene Formen von gleicher Determinante äquivalent sind oder nicht.*

II. *Alle Substitutionen zu finden, durch welche die eine von zwei gegebenen äquivalenten Formen in die andere übergeht.*

Es wird aber gut sein, die Beschäftigung mit diesen beiden Problemen dadurch zu motiviren, dass wir zeigen, wie die Theorie der *Darstellung* der Zahlen durch quadratische Formen vollständig auf dieselben zurückgeführt werden kann; und so schicken wir im Folgenden einige Hauptsätze dieser Theorie voraus.

Man nennt, wie schon im Anfang dieses Abschnittes erwähnt ist, eine ganze Zahl m *darstellbar* durch die quadratische Form (a, b, c), wenn es zwei ganze Zahlen r, s von der Beschaffenheit giebt, dass

$$ar^2 + 2brs + cs^2 = m \tag{1}$$

wird. Wir können uns aber zunächst auf solche Darstellungen (r, s) beschränken, in welchen die beiden darstellenden Zahlen r, s *relative Primzahlen* sind; denn ist δ der grösste gemeinschaftliche Divisor von r und s, so ist m nothwendig theilbar durch δ^2; setzt man nun $r = r'\delta$, $s = s'\delta$ und $m = m'\delta^2$, so wird m' offenbar durch die Form (a, b, c) dargestellt, wenn r' und s' als darstellende Zahlen genommen werden. Da nun die letztern relative Primzahlen sind, so erkennt man leicht, dass, sobald alle Darstellungen der Zahlen in relativen Primzahlen bekannt sind, hieraus die übrigen Darstellungen leicht gefunden werden können. Wir schliessen daher die letztern von unserer Betrachtung ganz aus, und setzen also fest, dass die darstellenden Zahlen r, s keinen gemeinschaftlichen Divisor haben.

Es sei nun (a, b, c) eine bestimmte Form, $D = b^2 - ac$ ihre Determinante, m eine bestimmte durch sie darstellbare Zahl, und r, s die darstellenden Zahlen. Da die letztern relative Primzahlen sind, so giebt es (nach §§. 22, 24) immer unendlich viele Paare von ganzen Zahlen ϱ, σ, welche der unbestimmten Gleichung ersten Grades

$$r\sigma - s\varrho = +1 \tag{2}$$

Genüge leisten. Wir wählen ein solches Paar aus, und transformiren die darstellende Form (a, b, c) durch die Substitution $\begin{pmatrix} r, \varrho \\ s, \sigma \end{pmatrix}$; da die vier Substitutions-Coefficienten der Gleichung (2) genügen, so ist die neu entstehende Form der gegebenen nothwendig äquivalent; beide haben daher dieselbe Determinante D. Führt man die Transformation wirklich aus, so ergiebt sich vermöge

der Gleichung (1), dass m der erste Coefficient der neuen Form wird; bezeichnen wir den zweiten mit n, so finden wir

$$n = ar\varrho + b(r\sigma + s\varrho) + cs\sigma. \tag{3}$$

Den dritten Coefficienten l brauchen wir nicht auszurechnen; denn da wir aus (2) schon wissen, dass die Determinante $n^2 - ml$ der neuen Form $= D$ ist, so ergiebt sich der dritte Coefficient

$$l = \frac{n^2 - D}{m}.$$

Die Form (a, b, c) geht also durch die Substitution $\begin{pmatrix} r, & \varrho \\ s, & \sigma \end{pmatrix}$ in die äquivalente Form (m, n, l) über. Da nun der letzte Coefficient der neuen Form nothwendig eine ganze Zahl, also $n^2 - D$ durch m theilbar ist, so folgt, dass D quadratischer Rest von m, und n eine Wurzel der Congruenz

$$z^2 \equiv D \pmod{m} \tag{4}$$

ist.

Sehen wir jetzt nach, was für Aenderungen eintreten, wenn wir statt der bestimmten Auflösung ϱ, σ der Gleichung (2) irgend eine andere ϱ', σ' wählen. Subtrahirt man die beiden Gleichungen

$$r\sigma - s\varrho = 1, \quad r\sigma' - s\varrho' = 1$$

von einander, so ergiebt sich

$$r(\sigma' - \sigma) = s(\varrho' - \varrho);$$

da nun r und s relative Primzahlen sind, so muss $\varrho' - \varrho$ durch r theilbar sein; nennen wir den Quotienten v, so folgt

$$\varrho' = \varrho + rv, \quad \sigma' = \sigma + sv;$$

alle denkbaren Auflösungen ϱ', σ' sind daher in diesen Formeln enthalten, in welchen v eine beliebige positive oder negative Zahl bedeutet; und umgekehrt jedem beliebigen Werthe von v entsprechen zwei Zahlen ϱ', σ', welche der Gleichung genügen. Dies gilt selbst dann noch, wenn eine der beiden Zahlen r, s gleich Null und folglich die andere $= \pm 1$ ist.

Transformiren wir nun die Form (a, b, c) durch eine solche

Substitution $\begin{pmatrix} r, & \varrho' \\ s, & \sigma' \end{pmatrix}$, so wird der erste Coefficient der neuen äquivalenten Form nothwendig wieder $= m$, der mittlere

$$n' = a r \varrho' + b(r\sigma' + s\varrho') + c s \sigma';$$

substituirt man hierin für ϱ', σ' die obigen Ausdrücke, so wird mit Berücksichtigung der Gleichung (1)

$$n' = n + mv, \quad \text{also} \quad n' \equiv n \pmod{m}. \qquad (5)$$

Hieraus folgt, dass alle Wurzeln n' der Congruenz (4), welche auf diese Weise aus einer Darstellung (r, s) der Zahl m durch die Form (a, b, c) abgeleitet werden können, die sämmtlichen Individuen einer und derselben Zahlclasse $\equiv n$ nach dem Modulus m sind, also nur eine und dieselbe Wurzel der Congruenz (4) bilden; jedes Individuum n' dieser Zahlclasse wird, wenn v alle ganzen Zahlen durchläuft, d. h. wenn man der Reihe nach alle Auflösungen der Gleichung (2) betrachtet, ein Mal und auch nur ein Mal erzeugt. Man sagt daher, die Darstellung (r, s) der Zahl *m gehöre* zu dieser Wurzel $\equiv n$ der Congruenz (4), weil durch den angegebenen Process nur diese und keine andere Wurzel derselben zum Vorschein kommt.

Fassen wir das Bisherige in der folgenden umgekehrten Betrachtung zusammen:

Erstens: Damit eine Zahl m darstellbar sei durch eine Form (a, b, c) von der Determinante D, ist erforderlich die Möglichkeit der Congruenz $z^2 \equiv D \pmod{m}$, d. h. dass D quadratischer Rest von m sei. — Denn wir haben gesehen, dass die Annahme der Darstellbarkeit mit Nothwendigkeit zu dieser Folgerung führt.

Zweitens: Ist dann n irgend eine Wurzel der Congruenz $z^2 \equiv D \pmod{m}$, und zwar $n^2 - D = ml$, so muss, wenn eine Darstellung von m durch die Form (a, b, c) existiren soll, welche zu dieser Wurzel n gehört, nothwendig die Form (a, b, c) der Form (m, n, l) aequivalent sein. — Denn wenn die Darstellung (r, s) zu der Wurzel gehört, von welcher n ein bestimmter Repräsentant ist, so giebt es, wie sich gezeigt hat, unter den sämmtlichen Lösungen der Gleichung $r\sigma - s\varrho = 1$ eine und nur eine solche, für welche der Ausdruck

$$a r \varrho + b(r\sigma + s\varrho) + c s \sigma$$

genau dem vorgeschriebenen Repräsentanten n der Wurzel gleich wird; und folglich ist dann $\begin{pmatrix} r, & \varrho \\ s, & \sigma \end{pmatrix}$ eine Substitution, durch welche (a, b, c) in (m, n, l) übergeht.

Hieraus sehen wir, dass vor der Behandlung der Darstellung das erste Problem der Theorie der Aequivalenz vollständig gelöst sein muss: zu entscheiden, ob zwei Formen (a, b, c) und (m, n, l) von gleicher Determinante D äquivalent sind oder nicht.

Drittens: Sind die Formen (a, b, c) und (m, n, l) wirklich äquivalent, und ist $\begin{pmatrix} r, & \varrho \\ s, & \sigma \end{pmatrix}$ irgend eine Substitution, durch welche die erstere in die letztere übergeht, so bilden der erste und dritte Coefficient derselben in der That eine Darstellung (r, s) der Zahl m durch die Form (a, b, c), welche zu der Wurzel n gehört; und indem man alle solche Substitutionen $\begin{pmatrix} r, & \varrho \\ s, & \sigma \end{pmatrix}$ sucht, findet man auch alle zur Wurzel n gehörigen Darstellungen der Zahl m durch die Form (a, b, c), und jede nur ein einziges Mal. — Denn ist $\begin{pmatrix} r, & \varrho \\ s, & \sigma \end{pmatrix}$ eine solche Substitution, also in Folge der Aequivalenz $r\sigma - s\varrho = +1$, so sind r und s relative Primzahlen; ferner ist dann $m = ar^2 + 2brs + cs^2$, also ist (r, s) eine Darstellung der Zahl m durch die Form (a, b, c), welche in Folge der Gleichungen

$$r\sigma - s\varrho = 1, \quad n = ar\varrho + b(r\sigma + s\varrho) + cs\sigma$$

zu derjenigen Wurzel der Congruenz $z^2 \equiv D \pmod{m}$ gehört, von welcher n ein Repräsentant ist. Sind ferner $\begin{pmatrix} r, & \varrho \\ s, & \sigma \end{pmatrix}$ und $\begin{pmatrix} r', & \varrho' \\ s' & \sigma' \end{pmatrix}$ zwei verschiedene solche Substitutionen, so ist ganz gewiss nicht gleichzeitig $r' = r$ und $s' = s$; denn sonst wäre $\varrho' = \varrho + rv$, $\sigma' = \sigma + sv$, folglich der mittlere Coefficient der neuen Form $= n + mv$ und also $v = 0$, da ja der mittlere Coefficient $= n$ ist; mithin wäre auch $\varrho' = \varrho$ und $\sigma' = \sigma$, und folglich wären die beiden Substitutionen gar nicht verschieden; also

entsprechen zwei verschiedenen Substitutionen $\begin{pmatrix} r, & \varrho \\ s, & \sigma \end{pmatrix}$ und $\begin{pmatrix} r', & \varrho' \\ s', & \sigma' \end{pmatrix}$ auch zwei verschiedene Darstellungen (r, s) und (r', s') der Zahl m; jede solche Darstellung wird also höchstens einmal erzeugt. Aber jede solche Darstellung (r, s), welche zu der Wurzel n gehört, wird auch wirklich erzeugt; denn ist (r, s) wirklich eine solche, so können, wie schon oben bemerkt ist, ϱ, σ stets so gewählt werden, dass (a, b, c) durch die Substitution $\begin{pmatrix} r, & \varrho \\ s, & \sigma \end{pmatrix}$ genau in die Form (m, n, l) übergeht, deren mittlerer Coefficient der vorgeschriebene Repräsentant n dieser Wurzel ist. — Um daher alle zu einer Wurzel n der Congruenz $z^2 \equiv D \pmod{m}$ gehörenden Darstellungen (r, s) der Zahl m durch die Form (a, b, c) zu finden, muss auch das zweite Problem der Theorie der Aequivalenz vollständig gelöst sein: alle Substitutionen $\begin{pmatrix} r, & \varrho \\ s, & \sigma \end{pmatrix}$ zu finden, durch welche eine Eorm (a, b, c) in eine ihr äquivalente Form (m, n, l) übergeht.

§. 60.

Nachdem wir uns in der vorhergehenden Digression davon überzeugt haben, dass in der That die Theorie der Darstellung vollständig auf die beiden im vorigen Paragraph erwähnten Probleme der Lehre von der Aequivalenz zurückgeführt werden kann, so wenden wir uns nun zu der Lösung derselben. Das erstere, zu erkennen, ob zwei Formen von gleicher Determinante äquivalent sind oder nicht, erfordert ganz verschiedene Methoden, je nachdem die Determinante positiv oder negativ ist; in beiden Fällen ist aber die Lösung von der Art, dass, wenn die Aequivalenz der beiden Formen erkannt wird, zu gleicher Zeit auch eine Transformation der einen in die andere gefunden wird. Da also bei zwei wirklich äquivalenten Formen immer eine solche Transformation durch die Lösung der ersten Aufgabe gefunden ist, so besteht das zweite Problem nur noch darin, aus *einer* solchen Transformation *alle andern* zu finden; und da die Lösung desselben zunächst nicht von dem Vorzeichen der Determinante abhängt,

sondern für positive wie für negative Determinanten Anfangs eine gleichmässige Behandlung zulässt, so stellen wir es dem andern voran.

Unsere Aufgabe ist also die, aus einer Substitution L, durch welche eine Form φ in eine äquivalente Form ψ übergeht, alle Substitutionen S zu finden, welche denselben Erfolg haben. Wir können dieselbe sogleich durch einige Bemerkungen bedeutend vereinfachen, indem wir sie auf den einfachsten Fall reduciren, in welchem beide Formen identisch sind. Denn gesetzt, wir kennen alle Substitutionen T, durch welche die Form φ in sich selbst übergeht, so geht φ offenbar durch alle Substitutionen TL — so bezeichnen wir die aus den successiven Substitutionen T und L zusammengesetzte Substitution — in die andere Form ψ über, wenn für T der Reihe nach die verschiedenen Substitutionen gesetzt werden, durch welche φ in sich selbst übergeht. Alle diese Substitutionen TL gehören also zu den gesuchten Substitutionen S. Jetzt behaupten wir auch umgekehrt, dass auf diese Weise alle Substitutionen S erzeugt werden, und jede nur ein einziges Mal; denn bezeichnen wir mit L' die inverse Substitution von L (durch welche also die Form ψ in die Form φ zurückkehrt), so ist jede in der Form SL' enthaltene Substitution eine solche, durch welche die Form φ in sich selbst übergeht, und gehört mithin zu den mit T bezeichneten Substitutionen, so dass wir $SL' = T$ setzen können. Da nun die aus L' und L zusammengesetzte Substitution $L'L = \begin{pmatrix}1, & 0\\ 0, & 1\end{pmatrix}$ ist, so folgt hieraus $SL'L = S = TL$, also wird wirklich jede Substitution S auf die angegebene Art erzeugt. Dass endlich jede Substitution S nur ein einziges Mal erzeugt wird, leuchtet hieraus ebenfalls ein; ist nämlich $TL = S$, so ist $T = SL'$, also ist die Substitution T, durch welche eine bestimmte Substitution S erzeugt wird, immer eine vollkommen bestimmte, so dass zwei verschiedene Substitutionen T auch zwei verschiedene Substitutionen S erzeugen.

Da also der Complex der Substitutionen S vollständig mit dem Complex der Substitutionen TL übereinstimmt, wo L die gegebene Substitution bedeutet, durch welche die Form φ in die äquivalente Form ψ übergeht, so kommt es nur noch darauf an, alle Substitutionen T zu finden; unser Problem ist daher auf das folgende zurückgeführt:

Alle Substitutionen zu finden, durch welche eine Form in sich selbst übergeht.

Wir beschränken uns bei der Lösung dieser Aufgabe auf sogenannte *ursprüngliche* oder *primitive* Formen φ oder (a, b, c), d. h. solche Formen, in welchen die drei Coefficienten a, b, c keinen gemeinschaftlichen Divisor haben, und wir dürfen uns dies ohne wesentliche Einschränkung der Allgemeinheit erlauben. Sind nämlich (a, b, c) und (a', b', c') irgend zwei äquivalente Formen, so erhellt aus den Formeln des §. 54, dass jeder gemeinschaftliche Theiler der drei Zahlen a, b, c auch gemeinschaftlicher Theiler der drei Zahlen a', b', c' ist; und da in Folge der Aequivalenz auch die Coefficienten a, b, c ganz ähnlich durch a', b', c' ausgedrückt werden können, so leuchtet ein, dass beide Gruppen von Coefficienten dieselben gemeinschaftlichen, also auch denselben grössten gemeinschaftlichen Theiler m haben. Jede Substitution, durch welche (a, b, c) in (a', b', c') übergeht, transformirt nun auch die ursprüngliche Form $\left(\frac{a}{m}, \frac{b}{m}, \frac{c}{m}\right)$ — deren Determinante $= \frac{D}{m^2}$ ist — in die ebenfalls ursprüngliche Form $\left(\frac{a'}{m}, \frac{b'}{m}, \frac{c'}{m}\right)$ und umgekehrt; wir brauchen uns daher nur mit ursprünglichen Formen zu beschäftigen. Die nicht ursprüngliche Form (a, b, c) heisst *derivirt* aus der ursprünglichen Form $\left(\frac{a}{m}, \frac{b}{m}, \frac{c}{m}\right)$.

Wir zerfällen ferner sämmtliche ursprüngliche Formen (a, b, c) in zwei *Arten*, je nach dem grössten gemeinschaftlichen Divisor σ der drei Zahlen a, $2b$, c, welcher entweder $= 1$ oder $= 2$ ist; denn ginge σ nicht in 2 auf, so hätten die Zahlen a, b, c einen grössern gemeinschaftlichen Divisor als 1, und folglich wäre die Form keine ursprüngliche. Ist mindestens einer der beiden äussern Coefficienten a und c ungerade, so ist $\sigma = 1$ und dann heisst (a, b, c) eine Form der *ersten Art* (*forma proprie primitiva* oder *forma propria* nach *Gauss*); sind die beiden äussern Coefficienten a und c gleichzeitig gerade, so ist $\sigma = 2$ und dann heisst (a, b, c) eine Form der *zweiten Art* (*forma improprie primitiva* oder *forma impropria* nach *Gauss*). Im letztern Fall ist nothwendig b ungerade (weil sonst die Form nicht ursprünglich wäre) und folglich die Determinante $D = b^2 - ac \equiv 1 \pmod{4}$. Wir behandeln

aber beide Fälle zugleich, indem wir den Buchstaben σ als Zeichen für den grössten gemeinschaftlichen Divisor von a, $2b$, c beibehalten.

§. 61.

Es sei nun $\begin{pmatrix}\lambda, \mu\\ \nu, \varrho\end{pmatrix}$ irgend eine Substitution, durch welche die ursprüngliche Form (a, b, c) der σten Art in sich selbst übergeht, so ist zunächst

$$\lambda\varrho - \mu\nu = 1 \tag{1}$$

und ferner (nach §. 54)

$$a\lambda^2 + 2b\lambda\nu + c\nu^2 = a; \tag{2}$$
$$a\lambda\mu + b(\lambda\varrho + \mu\nu) + c\nu\varrho = b; \tag{3}$$

da aus diesen drei Gleichungen schon folgt, dass (a, b, c) in eine äquivalente Form übergeht, deren erster und zweiter Coefficient a und b sind, so ist der letzte Coefficient c' der neuen Form wegen der Gleichheit der Determinanten nothwendig $= c$; und folglich drücken diese Gleichungen vollständig aus, dass $\begin{pmatrix}\lambda, \mu\\ \nu, \varrho\end{pmatrix}$ eine Substitution der verlangten Art ist (dies würde nicht ebenso vollständig geschehen, wenn man die Gleichung $\lambda\varrho - \mu\nu = 1$ durch die andere Gleichung $a\mu^2 + 2b\mu\varrho + c\varrho^2 = c$ ersetzen wollte; denn dann würde man rückwärts nur schliessen können, dass $\lambda\varrho - \mu\nu = \pm 1$ ist).

Wir behandeln diese drei Gleichungen mit den vier Unbekannten λ, μ, ν, ϱ auf folgende Weise.

Wird $\lambda\varrho$ durch $\mu\nu + 1$ ersetzt, so nimmt die Gleichung (3) die Form

$$a\lambda\mu + 2b\mu\nu + c\nu\varrho = 0$$

an; verbindet man hiermit die Gleichung (2) und eliminirt einmal $2b$, dann c, so erhält man unter Berücksichtigung der Gleichung (1) die beiden folgenden:

$$a\mu + c\nu = 0;\ a(\lambda - \varrho) + 2b\nu = 0.$$

Da a von 0 verschieden ist (weil sonst D eine Quadratzahl wäre), so kann man $\nu = a\psi$ setzen, wo ψ eine rationale (ganze oder gebrochene) Zahl bedeutet; hierdurch gehen die beiden letzten Gleichungen in die drei folgenden über

$$\nu = a\psi,\ \mu = -c\psi,\ \lambda - \varrho = -2b\psi;$$

schreibt man sie in der Form

$$\nu = \frac{a}{\sigma}\cdot\sigma\psi,\ \mu = -\frac{c}{\sigma}\cdot\sigma\psi,\ \lambda - \varrho = -\frac{2b}{\sigma}\cdot\sigma\psi,$$

so ergiebt sich, dass $\sigma\psi$ eine ganze Zahl sein muss; denn hätte diese Zahl, auf ihre kleinste Benennung gebracht, einen von 1 verschiedenen Nenner, so müsste derselbe, da ν, μ und $\lambda - \varrho$ ganze Zahlen sein sollen, nothwendig in jeder der drei Zahlen $\frac{a}{\sigma}$, $\frac{c}{\sigma}$ und $\frac{2b}{\sigma}$ aufgehen, was unmöglich ist, da diese den grössten gemeinschaftlichen Divisor 1 haben. Wir können daher

$$\nu = \frac{a}{\sigma}u,\ \mu = -\frac{c}{\sigma}u,\ \lambda - \varrho = -\frac{2b}{\sigma}u \tag{4}$$

setzen, worin u eine neue unbekannte, aber ganze Zahl bedeutet. Setzen wir diese Ausdrücke für μ und ν in die Gleichung (1), so erhalten wir

$$\lambda\varrho = -\frac{ac}{\sigma^2}\cdot u^2 + 1,$$

und hieraus in Verbindung mit dem vorstehenden Ausdruck für $\lambda - \varrho$ die Gleichung

$$(\lambda + \varrho)^2 = (\lambda - \varrho)^2 + 4\lambda\varrho = \frac{4(Du^2 + \sigma^2)}{\sigma^2}$$

oder

$$\left(\frac{\sigma(\lambda + \varrho)}{2}\right)^2 = Du^2 + \sigma^2.$$

Hieraus ergiebt sich, dass $\frac{\sigma(\lambda + \varrho)}{2}$ jedenfalls eine ganze Zahl sein muss, die wir mit t bezeichnen wollen, so dass

$$\lambda + \varrho = \frac{2}{\sigma} t \quad \text{und} \quad t^2 = Du^2 + \sigma^2 \tag{5}$$

ist.

Wir können die vorstehende Untersuchung mit Rücksicht auf (4) und (5) in Folgendem zusammenfassen:

Ist $\begin{pmatrix}\lambda, \varrho \\ \mu, \nu\end{pmatrix}$ *eine Substitution, durch welche die ursprüngliche Form (a, b, c) der* σ *ten Art und von der Determinante D in sich selbst übergeht, so ist stets*

$$\begin{aligned} \lambda &= \frac{t - bu}{\sigma}, \quad \mu = -\frac{cu}{\sigma} \\ \nu &= \frac{au}{\sigma}, \quad \varrho = \frac{t + bu}{\sigma} \end{aligned} \tag{I}$$

wo t, u zwei ganze Zahlen bedeuten, welche der unbestimmten Gleichung

$$t^2 - Du^2 = \sigma^2 \tag{II}$$

Genüge leisten.

Aber dieser Satz lässt sich auch umkehren:

Sind t, u zwei ganze der Gleichung (II) *genügende Zahlen, so sind die durch die Gleichungen* (I) *bestimmten Zahlen* $\lambda, \mu, \nu, \varrho$ *die ganzzahligen Coefficienten einer Substitution* $\begin{pmatrix}\lambda, \mu \\ \nu, \varrho\end{pmatrix}$, *durch welche die Form (a, b, c) in sich selbst übergeht.*

Dies ergiebt sich auf folgende Weise. Zunächst ist zu beweisen, dass $\lambda, \mu, \nu, \varrho$ auch dann ganze Zahlen werden, wenn $\sigma = 2$ ist (wenn $\sigma = 1$, versteht sich dies von selbst); da in diesem Fall a und c gerade sind, so sind ν und μ ganze Zahlen; da ferner b ungerade, und folglich $D = b^2 - ac \equiv 1 \pmod{4}$ ist, so sind irgend zwei der Gleichung $t^2 - Du^2 = 4$ genügende Zahlen t, u entweder beide gerade oder beide ungerade; in beiden Fällen sind $t - bu$ und $t + bu$ gerade, und folglich λ und ϱ ganze Zahlen.

Nachdem dieser erste Punct sichergestellt ist, findet man leicht durch wirkliche Substitution der Ausdrücke (I) unter Berücksichtigung der Gleichung (II), dass die drei Relationen (1), (2) und (3) identisch erfüllt sind, dass also in der That die Form (a, b, c) durch die Substitution $\begin{pmatrix}\lambda, \mu \\ \nu, \varrho\end{pmatrix}$ in sich selbst übergeht.

Aus jeder bekannten Substitution $\begin{pmatrix}\lambda, \mu \\ \nu, \varrho\end{pmatrix}$ kann daher (z. B.

durch die Gleichungen $t = \frac{\sigma(\lambda + \varrho)}{2}, \quad u = \frac{\sigma\nu}{a}\Big)$ eine Auflösung t, u der Gleichung (II) gefunden werden, und umgekehrt. Es ist aber wichtig, zu bemerken, dass zwei verschiedenen Substitutionen auch zwei verschiedene Auflösungen der Gleichung (II) entsprechen, und umgekehrt zwei verschiedenen Auflösungen der Gleichung (II) auch zwei verschiedene Transformationen der Form (a, b, c) in sich selbst. Denn die Relationen (I) sind derartig, dass gegebenen Werthen t, u ein und nur ein System von Werthen $\lambda, \mu, \nu, \varrho$, und umgekehrt gegebenen Werthen von $\lambda, \mu, \nu, \varrho$ ein und nur ein System von Werthen t, u entspricht.

Hiemit ist also unser Problem nicht vollständig gelöst, sondern nur auf das andere reducirt:

Alle ganzzahligen Auflösungen der unbestimmten Gleichung (II) *zu finden.*

Dieses letztere bietet nun nicht die geringste Schwierigkeit dar, sobald die Determinante D *negativ* ist. Wenn nämlich Δ ihr absoluter Werth, also $D = -\Delta$ ist, so hat die Gleichung (II)

$$t^2 + \Delta u^2 = \sigma^2$$

nur eine *endliche* Anzahl von Auflösungen t, u; und zwar ist

1) bei Formen der ersten Art ($\sigma = 1$) die Anzahl der Auflösungen der Gleichung

$$t^2 + \Delta u^2 = 1$$

immer $= 2$, sobald $\Delta > 1$ ist; diese Auflösungen sind offenbar

$$t = +1, \; u = 0 \quad \text{und} \quad t = -1, \; u = 0;$$

hieraus folgt, dass

$$\begin{pmatrix}1, & 0\\ 0, & 1\end{pmatrix} \quad \text{und} \quad \begin{pmatrix}-1, & 0\\ 0, & -1\end{pmatrix}$$

auch die beiden einzigen Substitutionen sind, durch welche eine ursprüngliche Form von negativer Determinante $-\Delta$ (wo $\Delta > 1$) und von der ersten Art in sich selbst übergeht. Im Fall $\Delta = 1$ ist aber die Anzahl der Auflösungen $= 4$; diese sind

$$t = 1, \; u = 0; \quad t = -1, \; u = 0;$$
$$t = 0, \; u = 1; \quad t = 0, \; u = -1;$$

und folglich sind

$$\begin{pmatrix}1, & 0\\0, & 1\end{pmatrix};\quad \begin{pmatrix}-1, & 0\\0, & -1\end{pmatrix}$$
$$\begin{pmatrix}-b, & -c\\+a, & +b\end{pmatrix};\quad \begin{pmatrix}+b, & +c\\-a, & -b\end{pmatrix}$$

die vier einzigen Substitutionen, durch welche eine Form (a, b, c), in welcher $b^2 - ac = -1$ ist, in sich selbst übergeht.

2) Bei Formen der zweiten Art, für welche $\sigma = 2$, $D \equiv 1 \pmod{4}$ und folglich $\Delta \equiv 3 \pmod{4}$, ist die Anzahl der Auflösungen der Gleichung

$$t^2 + \Delta u^2 = 4$$

stets $= 2$, so oft $\Delta > 3$; diese sind

$$t = 2,\ u = 0;\ \text{und}\ t = -2,\ u = 0;$$

die hieraus resultirenden Substitutionen

$$\begin{pmatrix}1, & 0\\0, & 1\end{pmatrix}\ \text{und}\ \begin{pmatrix}-1, & 0\\0, & -1\end{pmatrix}$$

sind die beiden einzigen, durch welche eine solche Form in sich selbst übergeht. Im Fall $\Delta = 3$ ist aber die Anzahl der Auflösungen $= 6$; diese sind

$$t = +2,\ u = 0;\ t = +1,\ u = +1;\ t = +1,\ u = -1;$$
$$t = -2,\ u = 0;\ t = -1,\ u = -1;\ t = -1,\ u = +1;$$

und die hieraus resultirenden Substitutionen

$$\begin{pmatrix}1, & 0\\0, & 1\end{pmatrix};\quad \begin{pmatrix}\frac{1}{2}(1-b), & -\frac{1}{2}c\\ \frac{1}{2}a, & \frac{1}{2}(1+b)\end{pmatrix};\quad \begin{pmatrix}-\frac{1}{2}(1+b), & -\frac{1}{2}c\\ \frac{1}{2}a, & -\frac{1}{2}(1-b)\end{pmatrix}$$
$$\begin{pmatrix}-1, & 0\\0, & -1\end{pmatrix};\quad \begin{pmatrix}-\frac{1}{2}(1-b), & \frac{1}{2}c\\ -\frac{1}{2}a, & -\frac{1}{2}(1+b)\end{pmatrix};\quad \begin{pmatrix}\frac{1}{2}(1+b), & \frac{1}{2}c\\ -\frac{1}{2}a, & \frac{1}{2}(1-b)\end{pmatrix}$$

sind die einzigen, durch welche eine Form (a, b, c), in welcher $b^2 - ac = -3$ und a und c gerade sind, in sich selbst übergeht.

§. 62.

Bei weitem schwieriger ist die Theorie der Gleichung (II) für den Fall einer *positiven* Determinante D, und hierin zeigt sich

zuerst die grosse Verschiedenheit in der Natur der Formen von positiver und derer von negativer Determinante. Wir lassen daher diese Untersuchung für jetzt fallen, um sie später (in §. 83) wieder aufzunehmen, nachdem das andere in §. 59 erwähnte Problem der Lehre von der Aequivalenz seine Lösung gefunden haben wird. Auch bei diesem stellt sich etwas Aehnliches heraus, indem es durchaus nothwendig wird, die Formen von positiver und negativer Determinante vollständig gesondert zu behandeln; und da auch hier die Formen von negativer Determinante weit weniger Schwierigkeiten darbieten, so behandeln wir diese zunächst.

Um den Gang der Untersuchung nicht zu unterbrechen, schicken wir eine Bemerkung voraus, welche sich gleichmässig auf Formen von positiver wie von negativer Determinante bezieht. Offenbar geht eine Form (a, b, a'), in welcher wir absichtlich den letzten Coefficienten nicht mit c, sondern mit a' bezeichnen, durch eine Substitution von der Form $\begin{pmatrix} 0, & 1 \\ -1, & \delta \end{pmatrix}$ in eine äquivalente Form über, deren Coefficienten

$$a', \quad b' = -b - a'\delta, \quad a'' = a + 2b\delta + a'\delta^2$$

sind; diese Form (a', b', a'') soll der Form (a, b, a') *nach rechts benachbart*, und ebenso soll die letztere (a, b, a') der andern (a', b', a'') *nach links benachbart* heissen. Das Charakteristische der Beziehung zweier solcher benachbarter Formen φ und φ' besteht erstens darin, dass sie dieselbe Determinante haben, zweitens, dass der letzte Coefficient a' der einen Form φ zugleich der erste Coefficient der andern Form φ' ist, drittens, dass die Summe ihrer mittlern Coefficienten $b + b'$ durch diesen gemeinschaftlichen Coefficienten a' theilbar ist. Denn haben zwei Formen φ und φ' diese drei Eigenschaften, und setzt man $b + b' = -a'\delta$, so geht in der That die Form φ durch die Substitution

$$\begin{pmatrix} 0, & 1 \\ -1, & \delta \end{pmatrix}$$

in eine neue Form über, deren erste beide Coefficienten a', b' mit denen der Form φ' übereinstimmen; und da die neue Form jedenfalls der Form φ äquivalent ist, also auch dieselbe Determinante wie φ und folglich auch wie φ' hat, so muss sie mit φ' identisch

sein. — Beiläufig ergiebt sich aus dieser Charakteristik des Begriffs auch folgender später (§. 77) zu benutzende Satz: Ist $('a, 'b, a)$ der Form (a, b, a') nach links benachbart, so ist $(a, 'b, 'a)$ der Form (a', b, a) nach rechts benachbart.

§. 63.

Wir wenden uns nun zu der Untersuchung, ob zwei gegebene Formen von gleicher *negativer* Determinante $D = -\Delta$ äquivalent sind oder nicht. Zunächst ist zu bemerken, dass die beiden äusseren Coefficienten a und c einer solchen Form

$$\varphi = ax^2 + 2bxy + cy^2$$

nothwendig gleiche Vorzeichen haben, da $ac = b^2 + \Delta$ ist; da ferner

$$a\varphi = (ax + by)^2 + \Delta y^2$$

ist, so zeigt sich, dass alle durch die Form φ darstellbaren Zahlen dasselbe Vorzeichen haben wie a und c. Sind daher (a, b, c) und (a', b', c') äquivalente Formen, so haben die äussern Coefficienten a', c' der letztern Form dasselbe Zeichen wie die der erstern. Da ferner aus der Aequivalenz dieser beiden Formen auch die der beiden Formen $(-a, -b, -c)$ und $(-a', -b', -c')$ folgt, so können wir uns im Folgenden auf die Betrachtung solcher Formen von negativer Determinante beschränken, in welchen die beiden äusseren Coefficienten das *positive* Vorzeichen haben.

Um nun über die Aequivalenz zweier Formen dieser Art zu entscheiden, vergleicht man sie nicht direct mit einander, sondern mit sogenannten *reducirten* Formen. Man nennt eine Form (A, B, C) von negativer Determinante (und positiven äussern Coefficienten) eine reducirte, wenn der letzte Coefficient C nicht kleiner ist als der erste A, und der erste A wieder nicht kleiner als der absolute Werth des doppelten mittlern Coefficienten $2B$, in Zeichen, wenn

$$C \geqq A \geqq 2(B)$$

ist, wo (B) den absoluten Werth von B bedeuten soll. Wir beweisen nun zunächst folgenden Satz:

Jede Form von negativer Determinante ist einer reducirten Form äquivalent.

Zu dem Zweck betrachte man die der gegebenen Form (a, b, a') nach rechts benachbarten Formen (a', b', a''); unter diesen wird es immer eine (bisweilen auch zwei) geben, in welchen wenigstens die eine Bedingung $a' \geqq 2(b')$ erfüllt ist. Denn unter allen mit $-b$ nach dem Modul a' congruenten Zahlen giebt es eine b', deren absoluter Werth am kleinsten, und zwar kleiner oder wenigstens nicht grösser als $\frac{1}{2}a'$ ist (falls a' gerade und $b \equiv \frac{1}{2}a'$ (mod. a') ist, würde es zwei solche Zahlen b' geben, nämlich $\pm \frac{1}{2}a'$), so dass jedenfalls $b' \equiv -b$ (mod. a') und ausserdem $2(b') \leqq a'$ ist. Ist b' auf diese Weise gefunden, und $b + b' = -a'\delta$, so geht die Form (a, b, a') durch die Substitution

$$\begin{pmatrix} 0, & 1 \\ -1, & \delta \end{pmatrix}$$

in die nach rechts benachbarte Form (a', b', a'') über, in welcher $2(b') \leqq a'$ ist. Wenn nun gleichzeitig sich herausstellt, dass $a' \leqq a''$ ist, so ist (a', b', a'') eine reducirte Form und der Process geschlossen. Findet sich aber, dass das Gegentheil

$$a' > a''$$

Statt findet, so ist (a', b', a'') noch keine reducirte Form. Mit dieser verfahre man ebenso wie mit (a, b, a'), d. h. man transformire sie in eine nach rechts benachbarte Form (a'', b'', a'''), in welcher $2(b'') \leqq a''$ ist; sobald dann gleichzeitig $a'' \leqq a'''$ ist, so ist (a'', b'', a''') reducirt, folglich der Process geschlossen; ist dies aber nicht der Fall, also

$$a'' > a''',$$

so setze man den Process in derselben Weise fort. Immer aber wird er nach einer *endlichen* Anzahl von Operationen schliessen; denn wäre dies nicht der Fall, so hätte man eine nie abbrechende Reihe von positiven ganzen Zahlen

$$a', a'', a''' \;.\;.\;.\; a^{(n)}, a^{(n+1)} \;.\;.\;.,$$

in welcher jede folgende mindestens um eine Einheit kleiner wäre, als die unmittelbar vorausgehende, was unmöglich ist, da es im-

mer nur eine endliche Anzahl ganzer positiver Zahlen giebt, welche kleiner sind als eine gegebene.

Auf diese Weise ist bewiesen, dass man endlich zu einer Form $(a^{(n)}, b^{(n)}, a^{(n+1)})$ gelangen muss, in welcher nicht nur $2(b^{(n)}) \leqq a^{(n)}$, sondern auch $a^{(n)} \leqq a^{(n+1)}$ ist.

Zugleich ergiebt sich jedesmal durch die wirkliche Ausführung der Operationen eine Substitution, welche aus den successiven Substitutionen von der Form

$$\begin{pmatrix} 0, & 1 \\ -1, & \delta \end{pmatrix}$$

zusammengesetzt ist, und durch welche die gegebene Form (a, b, a') in die ihr äquivalente reducirte Form $(a^{(n)}, b^{(n)}, a^{(n+1)})$ übergeht.

Nehmen wir als Beispiel die Form (200, 100, 51), deren Determinante $D = -200$ ist, so haben wir $b' \equiv -100 \pmod{51}$ zu setzen und finden hieraus $b' = 2$; die Substitution, durch welche die gegebene Form (200, 100, 51) transformirt werden muss, ist daher $\begin{pmatrix} 0, & 1 \\ -1, & -2 \end{pmatrix}$; da wir aber den ersten und zweiten Coefficienten a' und b' und die Determinante D kennen, so brauchen wir diese Transformation nicht wirklich auszuführen; sondern wir berechnen den letzten Coefficienten a'' durch die Formel

$$a'' = \frac{b'^2 - D}{a'};$$

in unserm Fall finden wir also

$$a'' = \frac{4 + 200}{51} = 4.$$

Die benachbarte Form ist daher (51, 2, 4); sie ist nicht reducirt, weil der letzte Coefficient kleiner ist als der erste. Wir wiederholen daher dieselbe Operation, indem wir $b'' \equiv -2$ (mod. 4) und folglich $b'' = \pm 2$ setzen, wo beide Zeichen zulässig sind; dann ergiebt sich die Substitution $\begin{pmatrix} 0, & 1 \\ -1, & -1 \end{pmatrix}$ oder

$\begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix}$, je nachdem das obere oder untere Zeichen genommen wird, und ausserdem

$$a''' = \frac{4 + 200}{4} = 51;$$

also ist die neue Form $(4, \pm 2, 51)$, und diese ist, mag man das obere oder das untere Zeichen wählen, reducirt. Ferner geht die gegebene Form $(200, 100, 51)$ durch die Substitution

$$\begin{pmatrix} 0, & 1 \\ -1, & -2 \end{pmatrix} \begin{pmatrix} 0, & 1 \\ -1, & -1 \end{pmatrix} = \begin{pmatrix} -1, & -1 \\ 2, & 1 \end{pmatrix}$$

in die Form $(4, 2, 51)$, dagegen durch die Substitution

$$\begin{pmatrix} 0, & 1 \\ -1, & -2 \end{pmatrix} \begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix} = \begin{pmatrix} -1, & 0 \\ 2, & -1 \end{pmatrix}$$

in die Form $(4, -2, 51)$ über. Man sieht aus diesem Beispiele, wie einfach der angegebene Algorithmus sich gestaltet.

§. 64.

Wir sehen ferner an dem eben behandelten Beispiele, dass eine und dieselbe Form zwei verschiedenen reducirten Formen äquivalent sein kann, woraus folgt, dass auch zwei verschiedene reducirte Formen unter einander äquivalent sein können. Da es von grosser Wichtigkeit ist, dies allgemein zu untersuchen, so stellen wir uns die Frage:

Wann sind zwei reducirte Formen (a, b, c) und (a', b', c') von gleicher negativer Determinante $D = -\varDelta$ einander äquivalent?

Zunächst ziehen wir einige Folgerungen aus den beiden Bedingungen

$$2(b) \leqq a, \quad a \leqq c,$$

welche ausdrücken, dass die Form (a, b, c) eine reducirte ist. Es ergiebt sich nämlich aus der erstern $4b^2 \leqq a^2$, aus der letztern $a^2 \leqq ac$, also auch $4b^2 \leqq ac$ oder $3b^2 \leqq ac - b^2$, folglich

$$(b) \leqq \sqrt{\tfrac{1}{3}\varDelta}.$$

Hieraus folgt weiter, dass $3ac = 3\Delta + 3b^2 \leqq 4\Delta$ und, da $a^2 \leqq ac$ ist, dass

$$a \leqq \sqrt{\tfrac{4}{3}\Delta}$$

ist.

Nehmen wir jetzt an, die beiden reducirten Formen (a, b, c), (a', b', c') seien äquivalent, so dürfen wir, ohne die Allgemeinheit zu beeinträchtigen, voraussetzen, dass

$$a' \leqq a$$

ist. Es sei nun $\begin{pmatrix}\alpha, & \beta \\ \gamma, & \delta\end{pmatrix}$ die Substitution, durch welche (a, b, c) in (a', b', c') übergeht, also

$$1 = \alpha\delta - \beta\gamma \tag{1}$$

$$a' = a\alpha^2 + 2b\alpha\gamma + c\gamma^2 \tag{2}$$

$$b' = a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta. \tag{3}$$

Multipliciren wir die Gleichung (2) mit a, so ergiebt sich

$$aa' = (a\alpha + b\gamma)^2 + \Delta\gamma^2;$$

da nun sowohl a, als auch $a' \leqq \sqrt{\tfrac{4}{3}\Delta}$, und also

$$aa' \leqq \tfrac{4}{3}\Delta$$

ist, so folgt, dass in der vorstehenden Gleichung γ^2 entweder $= 0$ oder $= 1$ sein muss; denn wäre $\gamma^2 \geqq 4$, so wäre $aa' \geqq 4\Delta$, was mit der Bedingung $aa' \leqq \tfrac{4}{3}\Delta$ streitet. Wir unterscheiden nun diese beiden Fälle:

I. $\gamma = 0$.

Dann lauten die drei obigen Gleichungen folgendermaassen:

$$\alpha\delta = 1;\ a' = a\alpha^2;\ b' = a\alpha\beta + b;$$

aus der ersten folgt $\alpha = \delta = \pm 1$; also ist $a' = a$, und die dritte Gleichung lehrt, dass $b' - b = \pm a\beta$ durch $a = a'$ theilbar ist; da nun aber $(b) \leqq \tfrac{1}{2}a$ und $(b') \leqq \tfrac{1}{2}a'$, also auch $(b') \leqq \tfrac{1}{2}a$ ist, so sind nur zwei Fälle möglich: entweder ist $b' - b = 0$, also $b' = b$ und folglich, da schon $a' = a$ ist, auch $c' = c$, d. h. die Formen sind identisch, in welchem Fall sich die Aequivalenz von selbst

versteht; oder es ist der absolute Werth von $b' - b$, da er unmöglich grösser als a sein kann und doch durch a theilbar sein muss, gleich a; in diesem Fall muss eine der beiden Zahlen b, b' gleich $+\frac{1}{2}a$, die andere gleich $-\frac{1}{2}a$, und also $c' = c$ sein; wir werden daher auf zwei nicht identische *formae ancipites* $(a, \frac{1}{2}a, c)$ und $(a, -\frac{1}{2}a, c)$ geführt. Diese sind aber in der That äquivalent, und die erstere geht in die letztere durch die Substitution $\begin{pmatrix}1, -1\\ 0, +1\end{pmatrix}$ über.

II. $\gamma = \pm 1$.

In diesem Fall lautet die Gleichung (2) folgendermaassen

$$a' = a\alpha^2 \pm 2b\alpha + c;$$

da wir angenommen haben, dass a' nicht grösser als a, und folglich auch nicht grösser als c ist, so folgt, dass

$$a\alpha^2 \pm 2b\alpha \leqq 0$$

ist. Da nun andererseits $2(b) \leqq a$ und stets $(\alpha) \leqq \alpha^2$, also auch der absolute Werth von $2b\alpha$ nicht grösser ist als $a\alpha^2$, so ist ganz gewiss

$$a\alpha^2 \pm 2b\alpha \geqq 0.$$

Es kann also $a\alpha^2 \pm 2b\alpha$ weder positiv noch negativ sein, und folglich ist

$$a\alpha^2 \pm 2b\alpha = 0,$$

also $a' = c$; da aber $a' \leqq a$ und $a \leqq c$, so folgt weiter, dass sowohl $a' = a$, als auch $c = a$ ist. Nun kann man die Gleichung (3) mit Hülfe der Gleichung (1) in die Form

$$b + b' = a\alpha\beta + 2b\alpha\delta \pm c\delta$$

bringen, und da $c = a$, und $2b\alpha = \mp a\alpha^2$ ist, so ergiebt sich

$$b + b' = a(\alpha\beta \mp \alpha^2\delta \pm \delta)$$

d. h. $b + b'$ ist theilbar durch a. Hieraus folgt ganz ähnlich wie im Fall I, dass $b + b'$ entweder $= 0$, oder dass der absolute Werth von $b + b'$ gleich a sein muss. Im letztern Fall müssten b und b' einander gleich, nämlich $= \pm\frac{1}{2}a$ sein, dann erhielte

man also wieder den Fall zweier identischen Formen, der kein Interesse darbietet. Im erstern Fall dagegen ist $b' = -b$, folglich da $a' = a$, und auch $c = a$ ist, auch $c' = c = a$; wir haben daher folgende zwei Formen (a, b, a) und $(a, -b, a)$, welche (wenn b von Null verschieden ist) nicht identisch sind; diese sind wirklich äquivalent, und die erstere geht in die letztere durch die Substitution $\begin{pmatrix} 0, & -1 \\ 1, & 0 \end{pmatrix}$ über.

Wir fassen das Resultat der Untersuchung in Folgendem zusammen:

Die beiden einzigen Fälle, in denen zwischen zwei nicht identischen reducirten Formen Aequivalenz Statt findet, sind die folgenden: die Formen $(a, \frac{1}{2}a, c)$ *und* (a, b, a) *gehen resp. durch die Substitutionen*

$$\begin{pmatrix} 1, & -1 \\ 0, & +1 \end{pmatrix} \textit{ und } \begin{pmatrix} 0, & -1 \\ 1, & 0 \end{pmatrix}$$

in die Formen $(a, -\frac{1}{2}a, c)$ *und* $(a, -b, a)$ *über.*

§. 65.

Hiermit ist nun auch die Aufgabe gelöst, zu entscheiden, ob zwei Formen von gleicher negativer Determinante äquivalent sind oder nicht. Sind φ und ψ die beiden Formen, so transformire man jede derselben, falls sie noch nicht reducirt sein sollte, nach der oben angegebenen Methode in eine reducirte Form, φ in φ', ψ in ψ'. Stellt sich dann heraus, dass φ' und ψ' identisch ausfallen, oder dass sie einen der beiden eben untersuchten Fälle darbieten, in welchen zwei nicht identische reducirte Formen dennoch äquivalent sind (was durch den Anblick der beiden Formen augenblicklich erkannt wird), so sind die gegebenen Formen φ und ψ gewiss äquivalent. Und zugleich ergiebt sich eine Substitution, durch welche die eine Form in die andere übergeht; denn durch den Process der Reduction ergeben sich Substitutionen S, durch welche φ in φ', und T, durch welche ψ in ψ' übergeht. Sind daher φ' und ψ' identisch, so geht, wenn T' die inverse Substitution von T bedeutet, die Form φ durch die zu-

sammengesetzte Substitution ST' in die Form ψ über. Sind dagegen φ' und ψ' nicht identisch, aber doch äquivalent, so ist, wie wir oben gesehen haben, immer eine Substitution U bekannt, durch welche φ' in ψ' übergeht; und dann geht φ durch die zusammengesetzte Substitution SUT' in ψ über.

Zeigt sich aber, dass die Formen φ' und ψ' nicht identisch sind, und dass sie auch keinen der beiden im vorigen Paragraph erwähnten particulären Fälle darbieten, sind also diese beiden reducirten Formen nicht äquivalent, so sind auch die beiden gegebenen Formen φ und ψ nicht äquivalent, wie unmittelbar aus §. 56 folgt.

Hiermit sind für negative Determinanten die beiden in §. 59 aufgestellten Probleme der Lehre von der Aequivalenz vollständig gelöst: soeben das erstere, welches darin besteht, über die Aequivalenz oder Nichtäquivalenz zweier gegebener Formen zu entscheiden; und zugleich haben wir jedesmal, wenn die Entscheidung für die erstere lautet, auch eine Substitution zu finden gelehrt, durch welche die eine Form in die andere übergeht. Das zweite Problem, aus einer gegebenen Substitution, durch welche eine gegebene Form in eine (hierdurch schon völlig bestimmte) äquivalente Form übergeht, alle Substitutionen zu finden, durch welche die erstere Form in dieselbe zweite Form übergeht, ist (für ursprüngliche Formen) in §. 61 ebenfalls vollständig gelöst.

§. 66.

Aus den vorhergehenden Untersuchungen über die Formen von negativer Determinante lässt sich eine Reihe von interessanten Folgerungen ableiten; bevor wir aber zu denselben übergehen, wollen wir eine Betrachtung anstellen, welche sich gleichmässig auf Formen von *negativer* und Formen von *positiver* Determinante bezieht, und welche in den künftigen Untersuchungen die grösste Rolle spielt.

Es sei f eine bestimmte gegebene Form von der Determinante D, und F der Inbegriff aller der Formen $f, f', f'' \ldots$, welche mit

f (eigentlich) äquivalent sind; da nun je zwei Formen, welche einer dritten Form äquivalent sind, auch unter einander äquivalent sind, so sind also je zwei in dem System F vorkommende Formen f', f'' einander äquivalent; ist daher f' irgend eine in F vorkommende Form, so ist das System aller mit f' äquivalenten Formen identisch mit dem System F. Ein solches System unter einander äquivalenter Formen soll eine *Classe von Formen* oder eine *Formenclasse* heissen, und es leuchtet ein, dass durch irgend ein Individuum einer solchen Classe alle andern derselben Classe angehörenden Formen vollständig bestimmt sind; man kann daher immer ein solches Individuum als *Repräsentanten der Formenclasse* ansehen.

Es würde nicht schwer sein zu beweisen, dass es in jeder solchen Formenclasse unendlich viele Individuen giebt, d. h. dass die Anzahl der Formen, in welche eine gegebene Form f durch die unendlich vielen verschiedenen Substitutionen $\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}$ übergeht, in denen $\alpha\delta - \beta\gamma = +1$, unendlich gross ist, obgleich es vorkommen kann, und zwar bei positiven Determinanten immer vorkommt, dass unendlich viele von diesen Substitutionen die Form f nur in eine und dieselbe Form f' transformiren; allein dieser Nachweis hat für uns zunächst kein Interesse. Von grösserer Wichtigkeit und von dem grössten Interesse ist dagegen die folgende Betrachtung.

Denkt man sich alle Formen von einer und derselben Determinante D in ihre verschiedenen Classen eingetheilt, und wählt man aus jeder Classe nach Belieben eine Form als Repräsentanten derselben, so erhält man ein sogenanntes *vollständiges System nicht äquivalenter Formen* für diese Determinante D; die fundamentale und vollständig charakteristische Eigenschaft eines solchen vollständigen Formensystems S besteht darin, dass jede beliebige Form von der Determinante D stets einer, aber auch nur einer von den in diesem System S enthaltenen Formen äquivalent ist. Die Anzahl dieser verschiedenen Classen (und also auch ihrer Repräsentanten in dem vollständigen Formensystem S) ist nun, wie sich zunächst für negative, später auch für positive Determinanten herausstellen wird, eine *endliche*, und wir bezeichnen absichtlich schon jetzt die genaue Bestimmung dieser Classenanzahl für eine gegebene Determinante, welche innig mit den schönsten algebraischen und analytischen Untersuchungen dieses Jahr-

hunderts verknüpft ist, als die letzte und hauptsächlichste von uns zu lösende Aufgabe.

§. 67.

Zunächst wollen wir uns aber auf Formen von *negativer* Determinante beschränken, und zwar wieder auf solche, deren äussere Coefficienten positiv sind. Da jede Form von negativer Determinante $D = -\varDelta$ einer reducirten Form und im Allgemeinen auch nur einer solchen reducirten Form äquivalent ist, so brauchen wir, um ein vollständiges Formensystem zu erhalten, nur die sämmtlichen reducirten Formen aufzusuchen und jedesmal, wenn zwei solche nicht identische Formen einen der beiden in §. 64 erwähnten Fälle darbieten, eine von ihnen nach Belieben fortzulassen, die andere beizubehalten. Dass die Anzahl der so übrig bleibenden nicht äquivalenten reducirten Formen endlich ist, ergiebt sich leicht aus den Bedingungen

$$2(b) \leqq a \leqq c,$$

denen eine reducirte Form (a, b, c) genügen muss, und der hieraus (in §. 64) gezogenen Folgerung

$$(b) \leqq \sqrt{\tfrac{1}{3}\varDelta}.$$

Bezeichnet man nämlich die grösste ganze in $\sqrt{\frac{1}{3}\varDelta}$ enthaltene Zahl mit λ (so dass $\lambda \leqq \sqrt{\frac{1}{3}\varDelta} < \lambda + 1$), so kann der mittlere Coefficient b keine andern, als die folgenden $2\lambda + 1$ Werthe

$$0, \ \pm 1, \ \pm 2 \ \ldots \ \pm \lambda$$

haben; und wenn man dem b irgend einen dieser Werthe beigelegt hat, so ist $ac = b^2 + \varDelta$; also hat man die Zahl $b^2 + \varDelta$ auf alle mögliche Arten in zwei positive Factoren zu zerlegen, und jedesmal denjenigen, welcher den andern an Grösse nicht übertrifft, für a, den letztern für c zu nehmen; stellt sich dann gleichzeitig heraus, dass $2(b) \leqq a$ ist, so ist die so gebildete Form wirklich eine reducirte und deshalb aufzuschreiben, im entgegengesetzten Fall aber fortzulassen. Auf diese Weise erhält man nothwendig alle reducirten Formen; ihre Anzahl ist aber nothwendig eine endliche, denn die Anzahl aller Zerlegungen der $(2\lambda + 1)$ Zahlen von

der Form $(b^2 + \Delta)$ in zwei Factoren ist selbst endlich. Wir haben daher das Resultat:

Die Anzahl aller nicht äquivalenten reducirten Formen von negativer Determinante, d. h. die Classenanzahl selbst ist endlich.

Beispiel 1: Für die Determinante $D = -12$ ist $\Delta = 12$; hieraus $\lambda = \sqrt{\frac{1}{3}\Delta} = 2$; wir haben daher b folgende Werthe durchlaufen zu lassen

$$0, \ \pm 1, \ \pm 2,$$

und dann die Zahlen $b^2 + \Delta$, d. h. die Zahlen

$$12, \ 13, \ 16$$

auf alle möglichen Arten in zwei Factoren zu zerlegen; es ist

$$12 = 1 \cdot 12 = 2 \cdot 6 = 3 \cdot 4$$
$$13 = 1 \cdot 13$$
$$16 = 1 \cdot 16 = 2 \cdot 8 = 4 \cdot 4.$$

Dies giebt, indem der erste Factor immer $= a$, der zweite $= c$ gesetzt wird, die eilf Formen

$$(1, 0, 12), \ (2, 0, 6), \ (3, 0, 4);$$
$$(1, \pm 1, 13);$$
$$(1, \pm 2, 16), \ (2, \pm 2, 8), \ (4, \pm 2, 4).$$

Von diesen sind die folgenden nicht reducirt

$$(1, \pm 1, 13), \ (1, \pm 2, 16), \ (2, \pm 2, 8),$$

weil in ihnen die Bedingung $2(b) \leqq a$ nicht erfüllt ist; als wirklich reducirte Formen bleiben daher nur die folgenden fünf übrig

$$(1, 0, 12), \ (2, 0, 6), \ (3, 0, 4), \ (4, \pm 2, 4);$$

allein die beiden Formen $(4, 2, 4)$ und $(4, -2, 4)$ gehören unter die Ausnahmefälle des §. 64, sind also äquivalent. Mithin enthält das vollständige Formensystem nur *vier* Formen, nämlich

$$(1, 0, 12), \ (2, 0, 6), \ (3, 0, 4), \ (4, 2, 4),$$

die als Repräsentanten ebenso vieler Classen gelten. Von diesen vier Formen sind nur die beiden folgenden

$$(1, 0, 12), \ (3, 0, 4)$$

ursprünglich, und zwar sind (da D nicht $\equiv 1 \pmod{4}$ ist) beide von der ersten Art.

Beispiel 2: Ist $D = -35$; also $\Delta = 35$, so ist $\lambda = 3$, also kann b nur die sieben Werthe

$$0, \quad \pm 1, \quad \pm 2, \quad \pm 3$$

durchlaufen; diesen entsprechen die Zahlen $b^2 + \Delta$:

$$35, \quad 36, \quad 39, \quad 44;$$

die Zerlegungen derselben in zwei Factoren sind folgende:

$$35 = 1 \cdot 35 = 5 \cdot 7$$
$$36 = 1 \cdot 36 = 2 \cdot 18 = 3 \cdot 12 = 4 \cdot 9 = 6 \cdot 6$$
$$39 = 1 \cdot 39 = 3 \cdot 13$$
$$44 = 1 \cdot 44 = 2 \cdot 22 = 4 \cdot 11.$$

Aber von den 22 entsprechenden Formen erfüllen nur die folgenden 10 die Bedingung $2(b) \leqq a$:

$$(1, 0, 35), \quad (5, 0, 7), \quad (2, \pm 1, 18)$$
$$(3, \pm 1, 12), \quad (4, \pm 1, 9), \quad (6, \pm 1, 6).$$

Da ferner die beiden Formen $(2, \pm 1, 18)$ den Fall I, die beiden Formen $(6, \pm 1, 6)$ den Fall II des §. 64 darbieten, so existiren nur *acht* nicht äquivalente reducirte Formen

$$(1, 0, 35), \quad (5, 0, 7), \quad (2, 1, 18)$$
$$(3, \pm 1, 12), \quad (4, \pm 1, 9), \quad (6, 1, 6);$$

diese sind alle ursprünglich; sechs, nämlich

$$(1, 0, 35), \quad (5, 0, 7), \quad (3, \pm 1, 12), \quad (4, \pm 1, 9)$$

sind von der ersten, die beiden andern

$$(2, 1, 18), \quad (6, 1, 6)$$

sind von der zweiten Art.

Beispiel 3: Ist $D = -48 = -\Delta$, so ist $\lambda = 4$, so dass b folgende Zahlen

$$0, \quad \pm 1, \quad \pm 2, \quad \pm 3, \quad \pm 4$$

durchlaufen muss; die Zerlegungen der entsprechenden Zahlen $b^2 + \Delta$ sind folgende:

$48 = 1 \cdot 48 = 2 \cdot 24 = 3 \cdot 16 = 4 \cdot 12 = 6 \cdot 8$
$49 = 1 \cdot 49 = 7 \cdot 7$
$52 = 1 \cdot 52 = 4 \cdot 13$
$57 = 1 \cdot 57 = 3 \cdot 19$
$64 = 1 \cdot 64 = 2 \cdot 32 = 4 \cdot 16 = 8 \cdot 8.$

Von den entsprechenden 25 Formen sind nur folgende eilf reducirt:

$$(1, 0, 48), \quad (2, 0, 24), \quad (3, 0, 16), \quad (4, 0, 12),$$
$$(6, 0, 8), \quad (7, \pm 1, 7), \quad (4, \pm 2, 13), \quad (8, \pm 4, 8).$$

Unter diesen besteht jedes der drei Paare $(7, \pm 1, 7)$, $(4, \pm 2, 13)$, $(8, \pm 4, 8)$ aus je zwei äquivalenten Formen; also bleiben nur *acht* nicht äquivalente Formen

$$(1, 0, 48), \quad (2, 0, 24), \quad (3, 0, 16), \quad (4, 0, 12),$$
$$(6, 0, 8), \quad (7, 1, 7), \quad (4, 2, 13), \quad (8, 4, 8).$$

Ursprünglich von der ersten Art sind die folgenden vier:

$$(1, 0, 48), \quad (3, 0, 16), \quad (7, 1, 7), \quad (4, 2, 13),$$

die andern vier sind derivirte Formen.

§. 68.

Um schon jetzt einen Begriff von der Fruchtbarkeit dieser Untersuchungen zu geben, verbinden wir in einigen Beispielen die gewonnenen Resultate mit der in §. 59 vorausgeschickten Theorie der Darstellung der Zahlen durch bestimmte quadratische Formen, bemerken jedoch gleich, dass die folgenden Sätze nur specielle Fälle eines grossen allgemeinen Satzes sind.

Die Formen der Determinante $D = -1$ bilden nur eine einzige Classe, denn es giebt für diese Determinante, wie man leicht erkennt, nur die einzige reducirte Form

$$(1, 0, 1) = x^2 + y^2.$$

Wir fragen nun nach dem System der durch diese Form darstellbaren, d. h. also in zwei Quadrate zerlegbaren Zahlen m; um aber die frühere Theorie unmittelbar anwenden zu können, lassen wir nur solche Darstellungen $x = r$, $y = s$ gelten, in denen die beiden darstellenden Zahlen r, s relative Primzahlen sind; ferner wollen

wir uns der Einfachheit halber auf ungerade darstellbare Zahlen m beschränken. Es sei also m eine solche darstellbare ungerade Zahl, so ist zunächst m positiv. Da ferner die Determinante -1 quadratischer Rest von m ist, so müssen alle in m aufgehenden Primzahlen von der Form $4h+1$ sein. Umgekehrt, ist diese Bedingung erfüllt, so ist die Determinante -1 quadratischer Rest von m, und die Congruenz

$$z^2 \equiv -1 \pmod{m}$$

hat im Ganzen (nach §. 37) 2^μ incongruente Wurzeln, wenn μ die Anzahl dieser von einander verschiedenen in m aufgehenden Primzahlen bedeutet (dies gilt selbst für den Fall, in welchem $\mu = 0$, $m = 1$ ist). Es sei n ein bestimmter Repräsentant einer bestimmten dieser Wurzeln, so bilde man die quadratische Form $\left(m, n, \frac{n^2+1}{m}\right)$ von der Determinante -1; da nur eine einzige Formenclasse existirt, so ist diese Form der reducirten Form $(1, 0, 1)$ nothwendig äquivalent, und man wird durch die in §. 65 angegebene Methode eine, und hieraus nach §§. 60, 61 alle Transformationen finden, durch welche $(1, 0, 1)$ in $\left(m, n, \frac{n^2+1}{m}\right)$ übergeht. Die Anzahl dieser von einander verschiedenen Transformationen $\begin{pmatrix} r, & \varrho \\ s, & \sigma \end{pmatrix}$ ist (nach §§. 60, 61) stets $= 4$; ebenso viele Darstellungen (r, s) der Zahl m existiren daher, welche zu derjenigen Wurzel gehören, deren Repräsentant n ist. Und da dasselbe Raisonnement auf jede der 2^μ Wurzeln der obigen Congruenz passt, so existiren im Ganzen

$$4 \cdot 2^\mu = 2^{\mu+2}$$

verschiedene Darstellungen der Zahl m.

Stellt man aber die Frage, auf wieviele verschiedene Arten eine solche Zahl m in zwei Quadrate zerlegt werden kann, ohne Rücksicht auf die Ordnung der beiden Quadrate und auf die Vorzeichen ihrer Wurzeln, so liefern je acht verschiedene Darstellungen von der Form

$$(x = \pm r,\ y = \pm s) \text{ und } (x = \pm s,\ y = \pm r)$$

nur eine einzige Zerlegung $m = r^2 + s^2$ (von diesen acht Darstellungen gehören vier, nämlich

$$(r, s),\ (-r, -s),\ (-s, r),\ (s, -r)$$

zu einer, und die andern vier

$$(r, -s),\ (-r, s),\ (-s, -r),\ (s, r)$$

zu der ihr entgegengesetzten Wurzel); folglich ist die Anzahl dieser verschiedenen Zerlegungen

$$= 2^{\mu-1},$$

mit einziger Ausnahme des Falles $m = 1$, weil dann nicht acht, sondern nur vier verschiedene Darstellungen

$$(x = \pm 1,\ y = 0) \text{ und } (x = 0,\ y = \pm 1)$$

existiren, die sich zu der einzigen Zerlegung $1 = 1^2 + 0^2$ vereinigen.

In diesem allgemeinen Resultat ist als specieller Fall der berühmte von *Fermat* aufgestellte, zuerst von *Euler* bewiesene Satz enthalten:

Jede (positive) Primzahl von der Form $4h + 1$ *lässt sich stets, und zwar nur auf eine einzige Weise in zwei Quadrate zerfällen.*

Die Bedingung, dass die Quadrate keinen gemeinschaftlichen Factor haben, fällt hier fort, da sie sich von selbst versteht.

Beispiel 1: Die Zahl 37 ist eine Primzahl von der Form $4h + 1$; die beiden Wurzeln der Congruenz $z^2 \equiv -1 \pmod{37}$ findet man (z. B. mit Hülfe des Wilson'schen Satzes) $\equiv \pm 6$; nimmt man $n = 6$, so hat man die Form (37, 6, 1) zu betrachten, welche durch die Substitution $\begin{pmatrix} 0, & +1 \\ -1, & -6 \end{pmatrix}$ in die reducirte Form (1, 0, 1) übergeht; umgekehrt geht also (1, 0, 1) durch die inverse Substitution $\begin{pmatrix} -6, & -1 \\ +1, & 0 \end{pmatrix}$ in (37, 6, 1) über. Also ist die gesuchte Zerlegung folgende: $37 = 6^2 + 1^2$; es ist nicht nöthig, die vier zu dieser Wurzel $+6$, und die andern vier zu der entgegengesetzten Wurzel -6 gehörenden Darstellungen hier einzeln aufzuschreiben.

Beispiel 2: Die Zahl $m = 65 = 5 \cdot 13$ ist das Product aus den beiden Primzahlen 5 und 13, welche beide die Form $4h + 1$ haben. Mithin giebt es $2^4 = 16$ verschiedene Darstellungen, also nur zwei verschiedene Zerlegungen der Zahl 65. Die vier Wur-

zeln der Congruenz $z^2 \equiv -1 \pmod{65}$ sind ± 8 und ± 18; wir bilden daher die beiden Formen (65, 8, 1) und (65, 18, 5), welche durch die Substitutionen $\begin{pmatrix} 0, & +1 \\ -1, & -8 \end{pmatrix}$ und $\begin{pmatrix} -1, & -2 \\ +4, & +7 \end{pmatrix}$ in die reducirte Form (1, 0, 1) übergehen; die inversen Substitutionen sind $\begin{pmatrix} -8, & -1 \\ +1, & 0 \end{pmatrix}$ und $\begin{pmatrix} +7, & +2 \\ -4, & -1 \end{pmatrix}$, und folglich sind die beiden gesuchten Zerlegungen folgende:

$$65 = 8^2 + 1^2 = 7^2 + 4^2.$$

§. 69.

Alle Formen der Determinante $D = -2$ bilden ebenfalls nur eine einzige Classe, da nur eine einzige reducirte Form

$$(1, 0, 2) = x^2 + 2y^2$$

vorhanden ist. Wir fragen auch hier wieder nach allen durch diese Form darstellbaren ungeraden Zahlen m; die erste Bedingung ist die, dass -2 quadratischer Rest von m sein muss; dazu ist erforderlich und hinreichend, dass für jede in m aufgehende (also ungerade) Primzahl p

$$\left(\frac{-2}{p}\right) = +1,$$

also p von einer der beiden Formen $8h + 1$ oder $8h + 3$ sei. Umgekehrt: sind die sämmtlichen μ in m aufgehenden Primzahlen p alle von der Form $8h + 1$ oder $8h + 3$, so hat die Congruenz

$$z^2 \equiv -2 \pmod{m}$$

stets 2^μ incongruente Wurzeln. Ist n ein bestimmter Repräsentant einer solchen Wurzel, so ist die Form $\left(m, n, \frac{n^2+2}{m}\right)$ nothwendig der Form (1, 0, 2) äquivalent; man findet daher (nach §. 65) eine Substitution $\begin{pmatrix} r, & \varrho \\ s, & \sigma \end{pmatrix}$, durch welche die letztere in die erstere übergeht; ausser dieser existirt (nach §. 61) nur noch die andere $\begin{pmatrix} -r, & -\varrho \\ -s, & -\sigma \end{pmatrix}$, welche dieselbe Eigenschaft hat; es giebt

daher zwei verschiedene Darstellungen (r, s) und $(-r, -s)$ der Zahl m, die zu dieser Wurzel gehören. Im Ganzen giebt es daher

$$2 \cdot 2^{\mu} = 2^{\mu+1}$$

verschiedene Darstellungen der Zahl m durch die Form $(1, 0, 2)$.

Man erkennt ferner leicht, dass, wenn die beiden Darstellungen $(\pm r, \pm s)$ zu der Wurzel n gehören, entsprechend die beiden Darstellungen $(\pm r, \mp s)$ zu der entgegengesetzten Wurzel $-n$ gehören. Je vier solche Darstellungen geben eine und dieselbe Zerlegung der Zahl m in ein Quadrat und ein doppeltes Quadrat; mithin ist die Anzahl aller verschiedenen Zerlegungen

$$= 2^{\mu-1};$$

die einzige Ausnahme bildet wieder der Fall, in welchem $\mu = 0$, also $m = 1$ ist; denn dann vereinigen sich die zwei verschiedenen Darstellungen ($+n$ ist $\equiv -n$ (mod. 1)) zu der einzigen Zerlegung $1 = 1^2 + 2 \cdot 0^2$. Der interessanteste specielle Fall ist wieder der, in welchem $\mu = 1$ ist:

Jede Primzahl p von einer der beiden Formen $8h + 1$ oder $8h + 3$ lässt sich stets und nur auf eine einzige Weise in ein Quadrat und ein doppeltes Quadrat zerlegen.

Beispiel 1: Ist $m = 41$, so ist die Bedingung erfüllt; μ ist $= 1$; die beiden Wurzeln der Congruenz $z^2 \equiv -2 \pmod{41}$ sind ± 11; die Form $(41, 11, 3)$ geht durch die Substitution

$$\begin{pmatrix} -1, & -1 \\ +4, & +3 \end{pmatrix}$$

in die Form $(1, 0, 2)$ über, diese also rückwärts in jene durch die Substitution $\begin{pmatrix} +3, & +1 \\ -4, & -1 \end{pmatrix}$; also ist $r = 3$, $s = -4$, und folglich

$$41 = 3^2 + 2 \cdot 4^2.$$

Beispiel 2: Ist $m = 33 = 3 \cdot 11$, so ist die Bedingung erfüllt; μ ist $= 2$, und folglich muss es zwei verschiedene Zerlegungen geben. Die Wurzeln der Congruenz $z^2 \equiv -2 \pmod{33}$ sind ± 8 und ± 14: wir bilden daher die beiden Formen

$$(33, 8, 2) \text{ und } (33, 14, 6),$$

welche resp. durch die Substitutionen

$$\begin{pmatrix}-1, & 0 \\ +4, & -1\end{pmatrix} \text{ und } \begin{pmatrix}-1, & +2 \\ +2, & -5\end{pmatrix}$$

in die Form (1, 0, 2) übergehen; die inversen Substitutionen sind

$$\begin{pmatrix}-1, & 0 \\ -4, & -1\end{pmatrix} \text{ und } \begin{pmatrix}-5, & -2 \\ -2, & -1\end{pmatrix},$$

und folglich ist

$$33 = 1^2 + 2 \cdot 4^2 = 5^2 + 2 \cdot 2^2.$$

§. 70.

Alle Formen der Determinante $D = -3$ bilden *zwei* Classen, als deren Repräsentanten man die reducirten Formen

$$(1, 0, 3) = x^2 + 3y^2$$

und

$$(2, 1, 2) = 2x^2 + 2xy + 2y^2$$

annehmen kann; sie sind resp. von der ersten und zweiten Art. Ungerade Zahlen können offenbar nur durch die erstere dargestellt werden; es sei daher m eine ungerade und der Einfachheit wegen durch 3 nicht theilbare Zahl; damit sie durch die Form (1, 0, 3) darstellbar sei, ist erforderlich, dass, wenn p irgend eine in ihr aufgehende Primzahl ist,

$$\left(\frac{-3}{p}\right) = +1,$$

folglich p von der Form $3h + 1$ sei. Umgekehrt, sobald diese Bedingung für alle μ in m aufgehenden Primzahlen p erfüllt ist, so hat die Congruenz

$$z^2 \equiv -3 \pmod{m}$$

stets 2^μ incongruente Wurzeln; ist n ein bestimmter Repräsentant einer solchen, so ist die Form $\left(m, n, \frac{n^2+3}{m}\right)$ von der ersten Art (da m ungerade ist) und folglich der Form (1, 0, 3) äquivalent. Es giebt also (nach §. 61) zwei Substitutionen

$$\begin{pmatrix}r, & \varrho \\ s, & \sigma\end{pmatrix} \text{ und } \begin{pmatrix}-r, & -\varrho \\ -s, & -\sigma\end{pmatrix}$$

durch welche die Form (1, 0, 3) in die Form $\left(m, n, \frac{n^2+3}{m}\right)$ übergeht, und folglich auch zwei Darstellungen (r, s) und $(-r, -s)$ der Zahl m, welche zu dieser Wurzel gehören. Im Ganzen giebt es daher

$$2 \cdot 2^\mu = 2^{\mu+1}$$

verschiedene Darstellungen einer solchen Zahl m durch die Form (1, 0, 3), die sich aber wieder auf nur

$$\tfrac{1}{4} \cdot 2^{\mu+1} = 2^{\mu-1}$$

verschiedene Zerlegungen der Zahl m in ein einfaches und ein dreifaches Quadrat reduciren (nur auf den Fall $\mu = 0$, also $m = 1$ passt die letztere Formel wieder nicht). Besonders bemerkenswerth ist der specielle Fall:

Jede Primzahl von der Form $3h + 1$ *ist stets und nur auf eine einzige Weise in ein einfaches und ein dreifaches Quadrat zerlegbar.*

Gehen wir nun zu den durch die zweite Form (2, 1, 2) darstellbaren, nothwendig geraden Zahlen über; wir beschränken uns auf diejenigen von der Form $2m$, in welcher wieder m eine ungerade und durch 3 nicht theilbare Zahl bedeutet. Dann erkennen wir leicht, dass der Complex dieser Zahlen m mit dem eben behandelten vollständig identisch ist. Denn aus der Möglichkeit der Congruenz $z^2 \equiv -3 \pmod{m}$ folgt auch die der Congruenz $z^2 \equiv -3 \pmod{2m}$, und umgekehrt (§. 37) und ausserdem ist die Anzahl der Wurzeln wieder $= 2^\mu$. Ist ferner n' ein bestimmter Repräsentant einer solchen, so ist die Form $\left(2m, n', \frac{n'^2+3}{2m}\right)$ nothwendig von der zweiten Art (denn der mittlere Coefficient n' ist ungerade, folglich $\frac{n'^2+3}{2m}$ gerade) und also gewiss der Form (2, 1, 2) äquivalent; man kann daher (nach §. 61) sechs verschiedene Transformationen der letztern Form in die erstere finden, welche in folgender Weise zusammenhängen:

$$\begin{pmatrix} r, & \varrho \\ s, & \sigma \end{pmatrix}, \begin{pmatrix} -s, & -\sigma \\ r+s, & \varrho+\sigma \end{pmatrix}, \begin{pmatrix} -r-s, & -\varrho-\sigma \\ r, & \varrho \end{pmatrix},$$
$$\begin{pmatrix} -r, & -\varrho \\ -s, & -\sigma \end{pmatrix}, \begin{pmatrix} s, & \sigma \\ -r-s, & -\varrho-\sigma \end{pmatrix}, \begin{pmatrix} r+s, & \varrho+\sigma \\ -r, & -\varrho \end{pmatrix};$$

hieraus ergeben sich entsprechend folgende sechs Darstellungen:

$$(r, s), \ (-s, r+s), \ (-r-s, r)$$
$$(-r, -s), \ (s, -r-s), \ (r+s, -r)$$

die alle zu derselben Wurzel n' gehören (die sechs zu der entgegengesetzten Wurzel $-n'$ gehörenden Darstellungen entstehen aus diesen durch Vertauschung der ersten darstellenden Zahl mit der zweiten). Im Ganzen existiren daher

$$6 \cdot 2^{\mu} = 3 \cdot 2^{\mu+1}$$

verschiedene Darstellungen der Zahl $2m$ durch die Form $(2, 1, 2)$, oder, was dasselbe ist, der Zahl m durch die Form $x^2 + xy + y^2$. Sieht man je vier zusammengehörige Darstellungen von der Form

$$(r, s), \ (-r, -s), \ (s, r), \ (-s, -r)$$

als nicht wesentlich verschieden an, so ist die Anzahl der wesentlich verschiedenen Darstellungen nur noch

$$= 3 \cdot 2^{\mu-1}.$$

Für eine Primzahl p von der Form $3h+1$ giebt es daher immer drei wesentlich verschiedene Darstellungen durch die Form $x^2 + xy + y^2$.

Beispiel: Ist $m = 13$; so sind $n = \pm 7$ die Wurzeln der Congruenz $z^2 \equiv -3 \pmod{26}$ und also auch der Congruenz $z^2 \equiv -3 \pmod{13}$. Wir bilden daher die beiden Formen

$$(13, 7, 4) \text{ und } (26, 7, 2).$$

Sie gehen resp. durch die Substitutionen

$$\begin{pmatrix} -1, & -1 \\ +2, & +1 \end{pmatrix} \text{ und } \begin{pmatrix} 0, & +1 \\ -1, & -4 \end{pmatrix}$$

in die Formen

$$(1, 0, 3) \text{ und } (2, 1, 2)$$

über. Die beiden inversen Substitutionen sind

$$\begin{pmatrix} +1, & +1 \\ -2, & -1 \end{pmatrix} \text{ und } \begin{pmatrix} -4, & -1 \\ +1, & 0 \end{pmatrix}$$

und folglich ist

$$13 = 1^2 + 3(-2)^2 = (-4)^2 + (-4) \cdot 1 + 1^2;$$

hieraus findet man leicht die beiden andern Darstellungen

$$13 = 4^2 + 4 \cdot (-3) + (-3)^2$$
$$= 3^2 + 3 \cdot 1 \quad + \quad 1^2$$

§. 71.

Als letztes Beispiel wählen wir die Determinante $D = -5$; es giebt *zwei* nicht äquivalente reducirte Formen

$$(1, 0, 5) \text{ und } (2, 1, 3),$$

beide sind ursprünglich und von der ersten Art. Wir suchen wieder das System aller ungeraden und durch 5 nicht theilbaren Zahlen m zu bestimmen, welche durch diese Formen darstellbar sind. Die dazu erforderliche Bedingung besteht darin, dass für jede in m aufgehende Primzahl p die Gleichung

$$\left(\frac{-5}{p}\right) = +1$$

Statt finden muss; hieraus folgt (§. 52, II), dass jede solche Primzahl von einer der vier Formen

$$20h + 1, \quad 20h + 9, \quad 20h + 3, \quad 20h + 7$$

sein muss. Ist diese Bedingung erfüllt, und μ die Anzahl der verschiedenen Primzahlen p, so hat die Congruenz

$$z^2 \equiv -5 \pmod{m}$$

wieder 2^μ incongruente Wurzeln; ist n ein bestimmter Repräsentant einer solchen, so ist die Form $\left(m, n, \frac{n^2+5}{m}\right)$ nothwendig einer und nur einer der beiden obigen reducirten Formen äquivalent; es giebt dann jedesmal (nach §. 61) zwei Substitutionen, durch welche diese reducirte Form in $\left(m, n, \frac{n^2+5}{m}\right)$ übergeht, also auch zwei zu der Wurzel n gehörige Darstellungen der Zahl m durch diese reducirte Form. Im Ganzen giebt es also

$$2 \cdot 2^\mu = 2^{\mu+1}$$

Darstellungen einer solchen Zahl durch die obigen reducirten

Formen. Allein es bleibt noch zweifelhaft, durch welche der beiden reducirten Formen die zu einer bestimmten Wurzel n gehörigen beiden Darstellungen erfolgen; und eine ähnliche Frage wird jedesmal da auftreten, wo es mehrere nicht äquivalente Formen derselben Art giebt. In unserm Fall ist es nicht schwierig, diesen Zweifel zu heben.

Ist nämlich die Zahl m darstellbar durch die Form (1, 0, 5), also z. B.

$$m = r^2 + 5s^2,$$

so folgt hieraus

$$m \equiv r^2 \pmod{5},$$

d.h. m ist quadratischer Rest von 5; ist dagegen die Zahl m darstellbar durch die zweite Form (2, 1, 3), also z. B.

$$m = 2r^2 + 2rs + 3s^2,$$

so ist

$$2m = (2r + s)^2 + 5s^2 \equiv (2r + s)^2 \pmod{5},$$

und, da 2 quadratischer Nichtrest von 5 ist, so ist m ebenfalls quadratischer Nichtrest von 5.

Es tritt also hier die besonders einfache Erscheinung auf, dass alle Darstellungen einer Zahl entweder nur durch die Form (1,0,5) oder nur durch die Form (2,1,3) geschehen, je nachdem m quadratischer Rest oder Nichtrest von 5, d. h. je nachdem $m \equiv \pm 1$, oder $\equiv \pm 2 \pmod{5}$ ist. Hieraus folgen die speciellen Sätze:

Jede Primzahl von einer der beiden Formen $20h + 1$, $20h + 9$ *ist auf vier Arten durch die Form* (1, 0, 5) *darstellbar (welche wesentlich nur eine einzige Zerlegung in ein einfaches und ein fünffaches Quadrat bilden); jede Primzahl von einer der beiden Formen* $20h + 3$, $20h + 7$ *ist auf vier Arten durch die Form* (2, 1, 3) *darstellbar.*

Beispiel 1: Ist $m = 29$, so sind $n = \pm 13$ die beiden Wurzeln der Congruenz $z^2 \equiv -5 \pmod{29}$; die hieraus gebildete Form (29, 13, 6) geht durch die Substitution

$$\begin{pmatrix} -1, & +1 \\ +2, & -3 \end{pmatrix}$$

in die reducirte Form (1, 0, 5) über; durch Umkehrung dieser Substitution erhält man die Zerlegung

$$29 = 3^2 + 5 \cdot 2^2.$$

Beispiel 2: Für $m = 27$ findet man $n = \pm 7$; die beiden entsprechenden Formen

$$(27, 7, 2) \text{ und } (27, -7, 2)$$

gehen bezüglich durch die Substitutionen

$$\begin{pmatrix} 0, & +1 \\ -1, & -4 \end{pmatrix} \text{ und } \begin{pmatrix} 0, & 1 \\ -1, & 3 \end{pmatrix}$$

in die reducirte Form (2, 1, 3) über; durch Umkehrung derselben erhält man daher die vier Darstellungen

$$27 = 2(\mp 4)^2 + 2(\mp 4)(\pm 1) + 3(\pm 1)^2$$
$$27 = 2(\pm 3)^2 + 2(\pm 3)(\pm 1) + 3(\pm 1)^2$$

von denen die beiden erstern zu der Wurzel $+ 7$, die beiden letztern zu der Wurzel $- 7$ gehören.

§. 72.

Wir wenden uns nun zu den Formen mit *positiver* Determinante D, um auch für sie die Hauptprobleme der Theorie der Aequivalenz zu lösen. Das zweite Problem (§. 59), aus *einer* Transformation einer Form in eine zweite *alle* Transformationen der erstern in die letztere zu finden, ist durch unsere frühere Untersuchung auf die Aufgabe zurückgeführt, alle ganzzahligen Auflösungen der Gleichung

$$t^2 - Du^2 = \sigma^2$$

zu finden. Dieselbe ist für positive Determinanten bei weitem schwieriger zu lösen, als für negative. Dasselbe gilt von dem ersten Hauptproblem: zu erkennen, ob zwei Formen von gleicher Determinante äquivalent sind oder nicht. Wir schlagen zur Lösung desselben einen ganz andern Weg ein, wie früher bei negativen Determinanten, einen Weg, der aber zugleich die Mittel an die Hand geben wird, auch die obige Gleichung vollständig aufzulösen.

Das Charakteristische dieser Methode besteht darin, dass wir auch *irrationale* Grössen in den Kreis unserer Betrachtungen ziehen. Ist nämlich (a, b, c) oder

$$ax^2 + 2bxy + cy^2$$

eine Form, deren Determinante $b^2 - ac = D$ positiv ist, so hat die entsprechende quadratische Gleichung

$$a + 2b\omega + c\omega^2 = 0$$

zwei reelle Wurzeln

$$\omega = \frac{-b \mp \sqrt{D}}{c},$$

die wir, je nachdem das obere oder untere Zeichen genommen wird, als die *erste* oder *zweite Wurzel der Form* (a, b, c) bezeichnen und von einander unterscheiden wollen, indem wir ein für alle Mal festsetzen, dass das Zeichen $\sqrt{D}$ stets die *positive* Quadratwurzel aus der Determinante bedeuten soll. Durch die Coefficienten der Form (a, b, c) ist also jede ihrer beiden Wurzeln vollständig, ohne Zweideutigkeit bestimmt. Aber umgekehrt ist auch jede Form (a, b, c) der Determinante D durch Angabe einer ihrer Wurzeln vollständig charakterisirt, in der Weise, dass zwei Formen (a, b, c) und (a', b', c') derselben Determinante D nothwendig identisch sind, sobald sie gleiche erste, oder gleiche zweite Wurzeln haben; denn aus der Gleichung

$$\frac{-b' \mp \sqrt{D}}{c'} = \frac{-b \mp \sqrt{D}}{c},$$

worin entweder die beiden obern, oder die beiden untern Zeichen zu nehmen sind, ergiebt sich in Folge der Irrationalität von $\sqrt{D}$ zunächst $c' = c$, und dann $b' = b$, also auch $a' = a$.

§. 73.

Wir wollen nun annehmen, es seien (a, b, c) und (a', b', c') zwei äquivalente Formen, und zwar wollen wir für einen Augenblick die uneigentliche Aequivalenz nicht ausschliessen, weil dadurch der Nerv der Betrachtung deutlicher hervortritt. Es sei $\binom{\alpha,\ \beta}{\gamma,\ \delta}$ eine Substitution, durch welche (a, b, c) in (a', b', c') übergeht, also

$$\alpha\delta - \beta\gamma = \pm 1.$$

Da durch diese Substitution

$$x = \alpha x' + \beta y', \quad y = \gamma x' + \delta y'$$

identisch

$$a x^2 + 2bxy + cy^2 = a'x'^2 + 2b'x'y' + c'y'^2$$

wird, so leuchtet ein, dass vermöge der Formeln

$$\omega = \frac{\gamma + \delta\omega'}{\alpha + \beta\omega'}, \quad \omega' = \frac{\gamma - \alpha\omega}{-\delta + \beta\omega} \tag{1}$$

aus einer Wurzel ω' der Form (a', b', c') eine Wurzel ω der Form (a, b, c) gefunden werden kann, und umgekehrt; denn die Wurzeln dieser Formen sind ja die Werthe der Verhältnisse $\frac{y}{x}$ und $\frac{y'}{x'}$, für welche die Formen verschwinden. Aber es fragt sich vor allen Dingen, ob zwei so verbundene Wurzeln ω und ω' gleichnamig (d. h. ob beide erste oder beide zweite Wurzeln) sind, oder nicht. Dazu müssen wir in der Gleichung

$$\omega' = \frac{\gamma - \alpha\omega}{-\delta + \beta\omega}$$

für die Wurzel ω ihren obigen Ausdruck durch die Coefficienten substituiren, wodurch wir zunächst

$$\omega' = \frac{\gamma c - \alpha(-b \mp \sqrt{D})}{-\delta c + \beta(-b \mp \sqrt{D})} = \frac{b\alpha + c\gamma \pm \alpha\sqrt{D}}{-b\beta - c\delta \mp \beta\sqrt{D}}$$

erhalten; machen wir den Nenner rational, indem wir den Bruch durch $-b\beta - c\delta \pm \beta\sqrt{D}$ erweitern, so ergiebt sich

$$\omega' = \frac{-(b\alpha + c\gamma)(b\beta + c\delta) + \alpha\beta D \mp (\alpha\delta - \beta\gamma) c\sqrt{D}}{(b\beta + c\delta)^2 - \beta^2 D}$$

$$= \frac{-(a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta) \mp (\alpha\delta - \beta\gamma)\sqrt{D}}{a\beta^2 + 2b\beta\delta + c\delta^2}$$

oder

$$\omega' = \frac{-b' \mp (\alpha\delta - \beta\gamma)\sqrt{D}}{c'}.$$

Ist daher $\alpha\delta - \beta\gamma = +1$, d. h. ist die Substitution eine eigentliche, so sind ω, ω' gleichnamige Wurzeln; ist dagegen $\alpha\delta - \beta\gamma = -1$, also die Substitution eine uneigentliche, so sind die beiden Wurzeln ω, ω' ungleichnamig, d. h. die eine ist eine erste, die andere eine zweite Wurzel.

Wir schliessen von jetzt an uneigentliche Aequivalenz und uneigentliche Substitutionen gänzlich aus; es sind dann also durch die Gleichungen (1) stets zwei *gleichnamige* Wurzeln der beiden äquivalenten Formen mit einander verbunden. Dieser Satz lässt sich in folgender Weise umkehren:

Wenn zwei Formen (a, b, c), (a', b', c') dieselbe Determinante D haben, und wenn zwei gleichnamige Wurzeln ω und ω' derselben durch die Gleichung

$$\omega = \frac{\gamma + \delta\omega'}{\alpha + \beta\omega'}$$

verbunden sind, in welcher die vier ganzen Zahlen $\alpha, \beta, \gamma, \delta$ der Gleichung

$$\alpha\delta - \beta\gamma = 1$$

genügen, so sind die beiden Formen äquivalent, und zwar geht die erstere durch die Substitution $\binom{\alpha,\ \beta}{\gamma,\ \delta}$ in die letztere über.

Denn setzt man wieder

$$\omega = \frac{-b \mp \sqrt{D}}{c},$$

so wird (da $\alpha\delta - \beta\gamma = +1$ ist)

$$\omega' = \frac{\gamma - \alpha\omega}{-\delta + \beta\omega} = \frac{-(a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta) \mp \sqrt{D}}{a\beta^2 + 2b\beta\delta + c\delta^2};$$

da nun andererseits

$$\omega' = \frac{-b' \mp \sqrt{D}}{c'}$$

und hierin, wegen der vorausgesetzten Gleichnamigkeit von ω und ω', das obere oder untere Zeichen zu nehmen ist, je nachdem in der Formel für ω, und also auch in der aus ihr abgeleiteten Formel für ω' das obere oder untere Zeichen gilt, so folgt, dass

$$c' = a\beta^2 + 2b\beta\delta + c\delta^2, \quad b' = a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta$$

ist. Diese beiden Gleichungen (in Verbindung mit $\alpha\delta - \beta\gamma = 1$) drücken aus, dass die Form (a, b, c) durch die Substitution $\binom{\alpha,\ \beta}{\gamma,\ \delta}$ in die äquivalente Form $\left(\frac{b'^2 - D}{c'}, b', c'\right)$ übergeht; der Voraussetzung nach hat aber die Form (a', b', c') dieselbe Determi-

nante wie (a, b, c); d. h. es ist $b'^2 - a'c' = D$; also ist diese Form, in welche (a, b, c) durch die Substitution $\binom{\alpha, \beta}{\gamma, \delta}$ übergeht, keine andere als (a', b', c'), was zu beweisen war.

Von besonderer Wichtigkeit für das Folgende ist die Betrachtung zweier benachbarter Formen (a, b, a') und (a', b', a''), in welchen der Definition zufolge (§. 62) die Summe $b + b'$ durch a' theilbar, also $b + b' = -a'\delta$ ist, und von welchen die erstere in die letztere durch die Substitution $\begin{pmatrix} 0, & 1 \\ -1, & \delta \end{pmatrix}$ übergeht. Die gleichnamigen Wurzeln ω und ω' dieser beiden Formen hängen durch die Gleichungen

$$\omega = \frac{-1 + \delta\omega'}{\omega'} = -\frac{1}{\omega'} + \delta$$

$$\omega' = \frac{-1}{-\delta + \omega} = \frac{1}{\delta - \omega}$$

zusammen.

§. 74.

Auch bei positiven Determinanten vergleicht man zwei Formen, deren Aequivalenz beurtheilt werden soll, nicht unmittelbar mit einander, sondern man transformirt jede von ihnen in eine sogenannte *reducirte* Form; der Begriff einer solchen ist aber hier wesentlich verschieden von demjenigen, welcher früher (§. 63) für negative Determinanten aufgestellt ist.

Eine Form (a, b, c) von positiver Determinante D heisst eine reducirte Form, wenn, abgesehen vom Zeichen, ihre erste Wurzel

$$\frac{-b - \sqrt{D}}{c} > 1,$$

ihre zweite Wurzel

$$\frac{-b + \sqrt{D}}{c} < 1$$

ist, und wenn ausserdem beide Wurzeln entgegengesetzte Zeichen haben.

Ziehen wir zunächst einige Folgerungen aus dieser Erklärung.

Da die erste Wurzel numerisch grösser als die zweite, also auch die Summe der beiden Grössen b und $\sqrt{D}$ numerisch grösser als ihre Differenz sein soll, so muss, da $\sqrt{D}$ positiv ist, auch b positiv sein (nicht $= 0$); da ferner die beiden Wurzeln entgegengesetzte Zeichen haben, so gilt dasselbe auch von den beiden Grössen

$$-(b + \sqrt{D}) \quad \text{und} \quad -b + \sqrt{D};$$

und da die erstere gewiss negativ ist, so muss die letztere positiv sein; es ist daher

$$0 < b < \sqrt{D}.$$

Bezeichnen wir ferner mit (c) wieder den absoluten Werth des Coefficienten c, so muss also im algebraischen Sinne (d. h. mit Rücksicht auf die Vorzeichen)

$$\frac{b + \sqrt{D}}{(c)} > 1 \quad \text{und} \quad 0 < \frac{-b + \sqrt{D}}{(c)} < 1,$$

d. h. es muss

$$0 < \sqrt{D} - b < (c) < \sqrt{D} + b$$

sein; und umgekehrt leuchtet ein, dass jede Form (a, b, c), deren Coefficienten diesen letztern Ungleichungen genügen, sicher eine reducirte Form ist, weil aus ihnen rückwärts die ursprünglichen Bedingungen sich ableiten lassen.

Aus der Definition ergeben sich noch weitere Folgerungen. Da $D = b^2 - ac$ und $b^2 < D$ ist, so müssen a und c entgegengesetzte Zeichen haben; da ferner die erste Wurzel und c ebenfalls entgegengesetzte Zeichen haben, so hat die erste Wurzel dasselbe Vorzeichen wie der erste Coefficient a der Form. Nun hat ferner die zweite Wurzel das entgegengesetzte Zeichen der ersten Wurzel, also dasselbe Vorzeichen wie der dritte Coefficient c der Form, was sich unmittelbar auch daraus ergiebt, dass $\sqrt{D} - b$ positiv ist.

Für den absoluten Werth des ersten Coefficienten a gelten dieselben Bedingungen, wie für den von c; denn da

$$D = b^2 + (a)(c),$$

also

$$(a) = \frac{(\sqrt{D} + b)(\sqrt{D} - b)}{(c)}$$

ist, so ergiebt sich aus den Bedingungen

$$\frac{\sqrt{D} + b}{(c)} > 1, \quad 0 < \frac{\sqrt{D} - b}{(c)} < 1,$$

dass

$$(a) > \sqrt{D} - b, \text{ und } (a) < \sqrt{D} + b$$

ist.

Für das Folgende ist noch der specielle Fall bemerkenswerth, in welchem

$$\sqrt{D} - (a) < b < \sqrt{D} \text{ und } (c) \geqq (a)$$

ist; aus diesen Bedingungen kann man nämlich stets schliessen, dass die Form (a, b, c) reducirt ist, obwohl die Umkehrung nicht gestattet ist. In der That, giebt man diesen Bedingungen die Form

$$0 < \sqrt{D} - b < (a) \lesseqqgtr (c),$$

so ergiebt sich zunächst, dass die zweite Wurzel

$$\frac{-b + \sqrt{D}}{c}$$

numerisch < 1, ferner dass die erste Wurzel

$$\frac{-b - \sqrt{D}}{c} = \frac{a}{\sqrt{D} - b}$$

numerisch > 1 ist. Hieraus folgt weiter, wie oben, dass b positiv ist, weil $\sqrt{D} + b$ numerisch grösser als $\sqrt{D} - b$ ist; und folglich haben, da ausserdem $b < \sqrt{D}$ ist, beide Wurzeln entgegengesetzte Zeichen. Also ist die Form gewiss eine reducirte.

§. 75.

Aus der Erklärung einer reducirten Form ergiebt sich ferner der folgende wichtige Satz:

Für jede positive Determinante giebt es nur eine endliche Anzahl reducirter Formen.

Denn, bezeichnen wir mit λ die grösste ganze in $\sqrt{D}$ enthaltene Zahl, so dass $\lambda < \sqrt{D} < \lambda + 1$ und also λ mindestens $= 1$ ist, so kann der mittlere Coefficient b einer reducirten Form (a, b, c) nur die λ verschiedenen Werthe $1, 2 \ldots \lambda$ haben; für jeden dieser Werthe von b ist $D - b^2 = (a)(c)$ auf alle mögliche Arten in zwei Factoren zu zerlegen, welche zwischen $\lambda - b$ und $\lambda + 1 + b$ exclusive (oder zwischen $\lambda + 1 - b$ und $\lambda + b$ inclusive) liegen; je zwei solchen Factoren a und c hat man entgegengesetzte Zeichen zu geben, und man muss sie permutiren, wenn sie ungleich sind. Dann sind aber wirklich alle reducirten Formen gefunden, und es giebt deren offenbar nur eine endliche Anzahl. —

Beispiel 1: Ist $D = 13$, so ist $\lambda = 3$; wir haben daher folgende Fälle und Zerlegungen:

$$b = 1;\quad 12 = 3 \cdot 4$$
$$b = 2;\quad 9 = 3 \cdot 3$$
$$b = 3;\quad 4 = 1 \cdot 4 = 2 \cdot 2$$

und diese liefern die folgenden 12 reducirten Formen:

$$(\pm 3, 1, \mp 4),\ (\pm 4, 1, \mp 3),\ (\pm 3, 2, \mp 3),$$
$$(\pm 1, 3, \mp 4),\ (\pm 4, 3, \mp 1),\ (\pm 2, 3, \mp 2).$$

Beispiel 2: Für $D = 19$ ist $\lambda = 4$; wir bilden daher folgende Tabelle:

$b = 1$; 18 giebt keine Zerlegung;
$$b = 2;\quad 15 = 3 \cdot 5;$$
$$b = 3;\quad 10 = 2 \cdot 5;$$
$$b = 4;\quad 3 = 1 \cdot 3;$$

hieraus ergeben sich folgende 12 reducirte Formen:

$$(\pm 3, 2, \mp 5),\ (\pm 2, 3, \mp 5),\ (\pm 1, 4, \mp 3),$$
$$(\pm 5, 2, \mp 3),\ (\pm 5, 3, \mp 2),\ (\pm 3, 4, \mp 1).$$

Beispiel 3: Für $D = 35$ ist $\lambda = 5$; also bilden wir die Tabelle

$b = 1$; 34 giebt keine Zerlegung;
$b = 2$; 31 " " "
$b = 3$; 26 " " "
$b = 4$; 19 " " "
$b = 5$; $10 = 1 \cdot 10 = 2 \cdot 5$;

wie erhalten daher 8 reducirte Formen:

$$(\pm 1, 5, \mp 10),\ (\pm 2, 5, \mp 5);$$
$$(\pm 10, 5, \mp 1),\ (\pm 5, 5, \mp 2).$$

Beispiel 4: Für $D = 79$ ist $\lambda = 8$; wir bilden daher folgende Tabelle:

$b = 1$; 78 giebt keine Zerlegung;
$b = 2$; 75 " " "
$b = 3$; $70 = 7 \cdot 10$;
$b = 4$; $63 = 7 \cdot 9$;
$b = 5$; $54 = 6 \cdot 9$;
$b = 6$; 43 giebt keine Zerlegung;
$b = 7$; $30 = 2 \cdot 15 = 3 \cdot 10 = 5 \cdot 6$;
$b = 8$; $15 = 1 \cdot 15 = 3 \cdot 5$;

wir erhalten daher 32 reducirte Formen:

$$(\pm 7, 3, \mp 10),\ (\pm 7, 4, \mp 9),\ (\pm 6, 5, \mp 9),\ (\pm 2, 7, \mp 15),$$
$$(\pm 3, 7, \mp 10),\ (\pm 5, 7, \mp 6),\ (\pm 1, 8, \mp 15),\ (\pm 3, 8, \mp 5),$$

und

$$(\pm 10, 3, \mp 7),\ (\pm 9, 4, \mp 7),\ (\pm 9, 5, \mp 6),\ (\pm 15, 7, \mp 2),$$
$$(\pm 10, 7, \mp 3),\ (\pm 6, 7, \mp 5),\ (\pm 15, 8, \mp 1),\ (\pm 5, 8, \mp 3).$$

§. 76.

Aehnlich wie bei negativen Determinanten (§. 63) beweisen wir auch die Richtigkeit des folgenden Satzes:

Jede Form von positiver Determinante ist einer reducirten Form äquivalent.

Bezeichnen wir die gegebene Form von positiver Determinante D mit (a, b, a'), so suchen wir eine ihr nach rechts benachbarte Form (a', b', a'') so zu bestimmen, dass

$$\sqrt{D} - (a') < b' < \sqrt{D}$$

wird. Da zufolge der Erklärung einer benachbarten Form der mittlere Coefficient b' jeden Werth erhalten kann, welcher $\equiv -b$ (mod. a') ist, und keinen andern, so fragt sich nur, ob zwischen den Grenzen $\sqrt{D}-(a')$ und $\sqrt{D}$ stets ein solcher Werth existirt; dies ist offenbar der Fall, da die sämmtlichen zwischen diesen beiden Grenzen enthaltenen ganzen Zahlen

$$\lambda+1-(a'),\ \lambda+2-(a')\ldots\lambda-1,\ \lambda$$

ein vollständiges Restsystem in Bezug auf den Modulus a' bilden; aus demselben Grunde ergiebt sich, dass nur eine einzige solche Zahl b' existirt. Nachdem b' bestimmt ist, geht die Form (a, b, a') durch die Substitution $\begin{pmatrix} 0, & +1 \\ -1, & -\frac{b+b'}{a'} \end{pmatrix}$ in die benachbarte Form (a', b', a'') über, deren Coefficienten a', b' der obigen Bedingung Genüge leisten. Findet sich nun, dass zu gleicher Zeit $(a'') \geqq (a')$ wird, so ist nach dem am Schluss des §. 74 besonders hervorgehobenen speciellen Fall die gefundene Form (a', b', a'') eine reducirte. Ist dagegen

$$(a') > (a''),$$

so verfahre man mit der gefundenen Form (a', b', a'') genau so wie mit der gegebenen Form, d. h. man bilde die ihr nach rechts benachbarte Form (a'', b'', a'''), in welcher

$$\sqrt{D}-(a'') < b'' < \sqrt{D}$$

ist, und welche gewiss eine reducirte ist, wenn $(a''') \geqq (a'')$ ist. Sollte aber wieder

$$(a'') > (a''')$$

sein, so setze man denselben Process in derselben Weise fort; da unter einer gegebenen positiven Zahl (a') nur eine endliche Anzahl von ganzen positiven Zahlen liegt, so muss man nach einer endlichen Anzahl von Transformationen durchaus zu einer Form $(a^{(n)}, b^{(n)}, a^{(n+1)})$ gelangen, in welcher sowohl

$$\sqrt{D}-(a^{(n)}) < b^{(n)} < \sqrt{D}$$

als auch

$$a^{(n+1)}) \geqq (a^{(n)})$$

ist, also zu einer reducirten Form gelangen, was zu beweisen war.

Es verdient bemerkt zu werden, dass bei diesem Process nicht gerade erst die letzte Form eine reducirte zu sein braucht, denn es giebt reducirte Formen, in welchen die Bedingungen des besondern hier benutzten speciellen Falles nicht erfüllt sind. Von grösserer Wichtigkeit ist es aber, besonders darauf aufmerksam zu machen, dass durch den angegebenen Process auch jedes Mal eine Substitution gefunden wird, durch welche die gegebene Form in die reducirte Form übergeht, und zwar erhält man diese Substitution durch Composition der successiven Substitutionen, welche in dem Process auftreten. Der Algorithmus selbst ist durchaus nicht beschwerlich, wie folgende Beispiele zeigen.

Beispiel 1: Die Form (4, 6, 7) hat die Determinante $D = 8$; es ist also $\lambda = 2$. Unter den Zahlen

$$-4, -3, -2, -1, 0, 1, 2$$

ist $b' = 1 \equiv -6 \pmod{7}$; dies giebt die benachbarte Form $(7, 1, -1)$, welche noch nicht reducirt ist. Da $(a'') = 1$ ist, so ist $b'' = \lambda = 2$, und folglich erhält man die benachbarte Form $(-1, 2, 4)$, welche wirklich reducirt ist. Durch die Substitution

$$\begin{pmatrix} 0, & +1 \\ -1, & -1 \end{pmatrix} \begin{pmatrix} 0, & 1 \\ -1, & 3 \end{pmatrix} = \begin{pmatrix} -1, & +3 \\ +1, & -4 \end{pmatrix}$$

geht die gegebene Form in die gefundene über.

Beispiel 2: Die Form (713, 60, 5) hat die Determinante $D = 35$; man findet nach der angegebenen Methode die nach rechts benachbarte Form $(5, 5, -2)$, und zu dieser wieder die Form $(-2, 5, 5)$, in welcher der letzte Coefficient in der That grösser ist als der erste. In diesem Beispiel ist aber auch schon die vorhergehende Form $(5, 5, -2)$ reducirt. Die gegebene Form geht durch die Substitution

$$\begin{pmatrix} 0, & +1 \\ -1, & -13 \end{pmatrix}$$

in $(5, 5, -2)$ und durch die Substitution

$$\begin{pmatrix} 0, & +1 \\ -1, & -13 \end{pmatrix} \begin{pmatrix} 0, & 1 \\ -1, & 5 \end{pmatrix} = \begin{pmatrix} -1, & +5 \\ 13, & -66 \end{pmatrix}$$

in $(-2, 5, 5)$ über.

Beispiel 3: Die Form (62, 95, 145), deren Determinante $D = 35$, geht durch die folgenden successiven Substitutionen

$$\begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix}, \begin{pmatrix} 0, & 1 \\ -1, & 2 \end{pmatrix}, \begin{pmatrix} 0, & 1 \\ -1, & 2 \end{pmatrix}, \begin{pmatrix} 0, & 1 \\ -1, & 4 \end{pmatrix}$$

successive in die Formen

$$(145, -95, 62),\ (62, -29, 13),\ (13, 3, -2),\ (-2, 5, 5)$$

über, von denen erst die letzte reducirt ist; die Zusammensetzung dieser Substitutionen giebt die Substitution $\begin{pmatrix} -3, & +10 \\ +2, & -7 \end{pmatrix}$, durch welche (62, 95, 145) in (— 2, 5, 5) übergeht.

§. 77.

Nachdem in den beiden vorhergehenden Paragraphen dargethan ist, dass jede Form von positiver Determinante einer reducirten Form äquivalent ist, und dass nur eine endliche Anzahl von reducirten Formen für jede gegebene Determinante existirt, so folgt hieraus unmittelbar:

Die Anzahl der Classen nicht äquivalenter Formen von positiver Determinante ist stets eine endliche.

Allein es bleibt noch die Hauptfrage zu beantworten, ob zwei nicht identische reducirte Formen derselben Determinante einander äquivalent sein können; denn erst dann haben wir (wie in §. 65 für negative Determinanten) die Mittel gewonnen, um über die Aequivalenz von zwei gegebenen Formen derselben positiven Determinante entscheiden zu können. Diese Untersuchung stösst bei positiven Determinanten auf bedeutende Schwierigkeiten, da in der That immer mehrere nicht identische und doch äquivalente reducirte Formen existiren.

Um einen sichern Boden für diese Untersuchung zu gewinnen, stellen wir zunächst die bestimmte Frage:

Kann eine reducirte Form (a, b, a') eine ihr nach rechts benachbarte Form (a', b', a'') haben, welche ebenfalls reducirt ist?

Nehmen wir einmal an, dies sei möglich, und es sei $\begin{pmatrix} 0, & 1 \\ -1, & \delta \end{pmatrix}$ die Substitution, durch welche die reducirte Form (a, b, a') in die ebenfalls reducirte Form (a', b', a'') übergeht. Sind dann ω und ω' zwei gleichnamige Wurzeln der ersten und der zweiten Form, so hängen diese (nach §. 73) durch die Gleichungen

$$\omega = -\frac{1}{\omega'} + \delta,\ \omega' = -\frac{1}{\omega - \delta} = \frac{1}{\delta - \omega}$$

mit einander zusammen. Wir wollen der Einfachheit halber festsetzen, dass ω und ω' die beiden *ersten* Wurzeln der beiden Formen bedeuten (obgleich dieselbe Relation auch zwischen den beiden zweiten Wurzeln Statt findet). Da in einer reducirten Form die beiden äussern Coefficienten entgegengesetzte Zeichen haben, und die erste Wurzel stets das Zeichen des ersten Coefficienten besitzt, so haben die beiden *unechten* Brüche ω und ω' bezüglich die Vorzeichen von a und a', also *entgegengesetzte* Vorzeichen, da der erste Coefficient a' der zweiten Form zugleich der letzte Coefficient der ersten Form ist. Wendet man dies auf die Gleichung

$$\omega' = \frac{1}{\delta - \omega} = -\frac{1}{\omega - \delta}$$

an, so ergiebt sich, dass $\omega - \delta$ ein echter Bruch sein muss von gleichem Vorzeichen wie ω; es muss daher δ diejenige vollständig bestimmte ganze Zahl sein, welche dem absoluten Werth nach nächst kleiner als ω ist und dem Vorzeichen nach mit ω übereinstimmt. Wir schliessen hieraus, dass eine reducirte Form (a, b, a') höchstens eine einzige nach rechts benachbarte Form (a', b', a'') hat, welche ebenfalls reducirt ist.

Aber es existirt auch wirklich immer eine solche der reducirten Form (a, b, a') nach rechts benachbarte und reducirte Form (a', b', a''). Denn es sei ω die erste Wurzel der reducirten Form (a, b, a'), also ein unechter Bruch, dessen Vorzeichen mit dem von a übereinstimmt; so wähle man die ganze Zahl δ so, dass ihr absoluter Werth (δ) die grösste ganze in (ω) enthaltene ganze Zahl (also nie $= 0$) wird, und gebe δ das Vorzeichen von ω; dann geht die gegebene Form (a, b, a') durch die so bestimmte Substitution $\begin{pmatrix} 0, & 1 \\ -1, & \delta \end{pmatrix}$ in eine benachbarte Form (a', b', a'') über, deren erste Wurzel

$$\omega' = -\frac{1}{\omega - \delta}$$

ein unechter Bruch ist, dessen Vorzeichen dem von ω und a entgegengesetzt ist und also mit dem von a' übereinstimmt. Bezeichnen wir nun mit ω_1 und ω'_1 die beiden zweiten Wurzeln, so besteht zwischen ihnen dieselbe Relation

$$\omega'_1 = \frac{1}{\delta - \omega_1};$$

da nun ω_1 ein echter Bruch ist, dessen Vorzeichen dem von ω, und also auch dem von δ entgegengesetzt, und da δ eine von Null verschiedene ganze Zahl ist, so folgt, dass $\delta - \omega_1$ ein unechter Bruch, und also ω'_1 ein echter Bruch ist, dessen Vorzeichen mit dem von δ, ω und a übereinstimmt, also dem von ω' und a' entgegengesetzt ist. Es ist also bewiesen, dass die beiden Wurzeln ω' und ω'_1 der neuen Form (a', b', a'') entgegengesetzte Zeichen haben, ferner dass die erste ω' ein unechter, die zweite ω'_1 ein echter Bruch ist; folglich ist diese Form in der That eine reducirte, was zu beweisen war.

Jede reducirte Form hat daher eine und nur eine nach rechts benachbarte Form, welche ebenfalls reducirt ist, und diese kann auf die angegebene Weise immer leicht gefunden werden.

Genau ebenso liesse sich nun auch beweisen, dass jede reducirte Form eine und nur eine nach links benachbarte reducirte Form besitzt. Doch ist es bequemer, diesen Fall auf den eben behandelten durch die einleuchtende Bemerkung zurückzuführen, dass die beiden Formen (a, b, a') und (a', b, a) gleichzeitig reducirte, oder gleichzeitig nicht reducirte Formen sind. Hieraus folgt nämlich in Verbindung mit einem früher (§. 62) erwähnten Satze, dass, wenn die reducirte Form (a, b, a') eine nach links benachbarte und ebenfalls reducirte Form $('a, 'b, a)$ besitzt, die reducirte Form (a', b, a) die nach rechts benachbarte Form $(a, 'b, 'a)$ hat, welche ebenfalls reducirt ist; und umgekehrt, sobald die Form $(a, 'b, 'a)$ der reducirten Form (a', b, a) nach rechts benachbart und zugleich reducirt ist, so ist die Form $('a, 'b, a)$ ebenfalls reducirt und der Form (a, b, a') nach links benachbart. Da wir nun gesehen haben, dass eine reducirte Form (a', b, a) immer eine und nur eine nach rechts benachbarte reducirte Form $(a, 'b, 'a)$ hat, so folgt:

Jede reducirte Form (a, b, a') *besitzt stets eine und nur eine nach links benachbarte reducirte Form* $('a, 'b, a)$.

§. 78.

Aus den soeben bewiesenen Sätzen über die nach rechts und links benachbarten reducirten Formen ergiebt sich, dass man

sämmtliche reducirte Formen einer positiven Determinante D in *Perioden* eintheilen kann, die auf folgende Weise zu bilden sind. Man wähle irgend eine reducirte Form φ_0 und bilde die nach rechts und links fortgesetzte Reihe

$$\ldots \varphi_{-2}, \varphi_{-1}, \varphi_0, \varphi_1, \varphi_2 \ldots$$

der successiven nach rechts und nach links benachbarten reducirten Formen, welche durch das eine Glied φ_0 vollständig bestimmt sind. Da es nur eine endliche Anzahl von reducirten Formen der Determinante D giebt, und die ersten Coefficienten zweier auf einander folgenden Formen stets entgegengesetzte Zeichen haben, so muss einmal auf eine Form φ_μ dieser Reihe nach einer geraden Anzahl $2n$ von Gliedern eine mit φ_μ identische Form $\varphi_{\mu+2n}$ folgen; und da eine Form φ_μ oder $\varphi_{\mu+2n}$ nur eine einzige nach rechts, und nur eine einzige nach links benachbarte reducirte Form besitzt, so müssen auch die beiden Formen, $\varphi_{\mu+1}$ und $\varphi_{\mu+1+2n}$, ebenso die beiden Formen $\varphi_{\mu-1}$ und $\varphi_{\mu-1+2n}$, und also auch allgemein je zwei Formen dieser Reihe identisch sein, deren Indices dieselbe Differenz $2n$ haben. In der ganzen Reihe sind daher höchstens $2n$ verschiedene Formen

$$\varphi_0, \varphi_1, \varphi_2 \ldots \varphi_{2n-2}, \varphi_{2n-1};$$

und diese werden in der That alle von einander verschieden sein, wenn keine der Formen $\varphi_2, \varphi_4 \ldots \varphi_{2n-2}$ mit φ_0 identisch ist; denn wären φ_ν und $\varphi_{\nu+2n'}$ zwei identische Formen, so müsste auch $\varphi_{2n'}$ mit φ_0 identisch sein. Nehmen wir also an, dass $2n$ die Anzahl der wirklich verschiedenen Formen dieser Reihe ist, so besteht dieselbe aus einer nach beiden Seiten sich unendlich oft periodisch wiederholenden Folge dieser $2n$ Formen; je zwei Formen φ_μ und φ_ν, deren Indices eine durch $2n$ theilbare Differenz $\mu - \nu$ haben, sind identisch; und umgekehrt, sind die Formen φ_μ und φ_ν identisch, so ist $\mu \equiv \nu$ (mod. $2n$).

Es kann nun sein, dass diese $2n$ Formen alle reducirten Formen der Determinante D erschöpfen; aber es ist auch möglich, dass ausser ihnen noch andere reducirte Formen derselben Determinante existiren. Im letztern Fall sei ψ_0 eine solche, in der obigen Periode nicht enthaltene reducirte Form, so entspricht ihr ebenso eine Periode von $2m$ unter einander verschiedenen Formen

$$\psi_0, \psi_1, \psi_2 \ldots \psi_{2m-2}, \psi_{2m-1};$$

alle diese Formen der zweiten Periode werden auch von denen der ersten verschieden sein; denn besässen beide Perioden eine gemeinschaftliche Form, so wären beide Reihen vollständig identisch, da von dieser gemeinschaftlichen Form aus die Reihe nur auf eine einzige Weise nach rechts und links fortgesetzt werden kann.

In derselben Weise kann man fortfahren, bis endlich alle reducirte Formen in verschiedene Perioden eingetheilt sind; die Anzahl der Perioden ist nothwendig eine endliche; die Anzahl der Glieder kann in verschiedenen Perioden verschieden sein, jedenfalls ist sie stets gerade.

Beispiel 1: Wir haben (§. 75) das System der reducirten Formen für die Determinante $D = 13$ aufgestellt; nehmen wir z. B. für φ_0 die Form $(3, 1, -4)$, so erhalten wir folgende Periode von zehn Formen

$$\begin{aligned}
\varphi_0 &= (3, 1, -4); \ \varphi_1 = (-4, 3, 1);\\
\varphi_2 &= (1, 3, -4); \ \varphi_3 = (-4, 1, 3);\\
\varphi_4 &= (3, 2, -3); \ \varphi_5 = (-3, 1, 4);\\
\varphi_6 &= (4, 3, -1); \ \varphi_7 = (-1, 3, 4);\\
\varphi_8 &= (4, 1, -3); \ \varphi_9 = (-3, 2, 3).
\end{aligned}$$

Diese Rechnung geschieht am einfachsten auf folgende Art; um aus der reducirten Form (a, b, a') die ihr nach rechts benachbarte reducirte Form (a', b', a'') zu finden, braucht man nur ihren mittlern Coefficienten b' zu suchen, welcher durch die Congruenz $b' \equiv -b \pmod{a'}$ und die Nebenbedingungen

$$\lambda + 1 - (a') \leqq b' \leqq \lambda$$

stets vollständig bestimmt ist und durch den blossen Anblick der Formen sogleich erkannt wird. In unserm Fall ist $\lambda = 3$; man findet daher den mittlern Coefficienten b' der Form φ_1 durch die Bedingungen

$$b' \equiv -1 \pmod{4}, \quad 0 \leqq b' \leqq 3,$$

nämlich $b' = 3$. Und nachdem so b' gefunden ist, ergiebt sich

$$a'' = \frac{b'^2 - D}{a'},$$

also in unserm Fall $a'' = 1$. In derselben Weise ist fortzufahren, bis die erste Form φ_0 sich reproducirt; in unserm Beispiel wird der mittlere Coefficient von φ_{10} dadurch bestimmt, dass er $\equiv -2 \pmod{3}$ sein, und ausserdem nicht ausserhalb der Grenzen 1 und 3 liegen muss, woraus folgt, dass er $= 1$ ist; also wird φ_{10} identisch mit φ_0.

Die so gefundenen zehn ursprünglichen Formen der ersten Art erschöpfen aber noch nicht alle reducirten Formen der Determinante 13; es bleiben noch zwei ursprüngliche Formen der zweiten Art übrig

$$\psi_0 = (2, 3, -2), \quad \psi_1 = (-2, 3, 2)$$

welche offenbar noch eine zweite Periode bilden.

Beispiel 2: Für $D = 19$ erhalten wir folgende zwei Perioden, jede von sechs Gliedern:

$$\begin{array}{ll} \varphi_0 = (3, 2, -5); & \varphi_1 = (-5, 3, 2) \\ \varphi_2 = (2, 3, -5); & \varphi_3 = (-5, 2, 3) \\ \varphi_4 = (3, 4, -1); & \varphi_5 = (-1, 4, 3) \end{array}$$

und

$$\begin{array}{ll} \psi_0 = (5, 2, -3); & \psi_1 = (-3, 4, 1) \\ \psi_2 = (1, 4, -3); & \psi_3 = (-3, 2, 5) \\ \psi_4 = (5, 3, -2); & \psi_5 = (-2, 3, 5). \end{array}$$

Beispiel 3: Für $D = 35$ erhält man folgende vier Perioden, jede von zwei Gliedern:

$$\begin{array}{ll} \varphi_0 = (1, 5, -10), & \varphi_1 = (-10, 5, 1) \\ \psi_0 = (10, 5, -1), & \psi_1 = (-1, 5, 10) \\ \chi_0 = (2, 5, -5), & \chi_1 = (-5, 5, 2) \\ \theta_0 = (5, 5, -2), & \theta_1 = (-2, 5, 5). \end{array}$$

Beispiel 4: Die 32 reducirten Formen der Determinante $D = 79$ zerfallen in vier Perioden von je sechs Gliedern und zwei Perioden von je vier Gliedern; eine der sechsgliedrigen Perioden ist folgende:

$$\begin{array}{ll} \varphi_0 = (7, 3, -10); & \varphi_1 = (-10, 7, 3) \\ \varphi_2 = (3, 8, -5); & \varphi_3 = (-5, 7, 6) \\ \varphi_4 = (6, 5, -9); & \varphi_5 = (-9, 4, 7); \end{array}$$

aus ihr entstehen die drei andern durch Vertauschung der äussern Coefficienten (womit die Vertauschung von rechts und links in der Folge der Glieder verbunden ist), ferner durch Verwandlung der Vorzeichen der äussern Coefficienten in die entgegengesetzten. Eine der beiden viergliedrigen Perioden ist

$$\psi_0 = (1, 8, -15);\quad \psi_1 = (-15, 7, 2)$$
$$\psi_2 = (2, 7, -15);\quad \psi_3 = (-15, 8, 1);$$

aus ihr entsteht die andere durch die Zeichenänderung der äussern Coefficienten.

§. 79.

Die vorhergehenden Untersuchungen über die Perioden der reducirten Formen von positiver Determinante stehen in der engsten Beziehung zu der Entwicklung der Wurzeln dieser Formen in Kettenbrüche. Nehmen wir für die Anfangsform φ_0 einer Periode immer eine solche, deren erster Coefficient *positiv* ist, so ist auch ihre *erste* Wurzel ω_0 positiv. Wir bezeichnen mit ω_μ die *erste* Wurzel der Form φ_μ, mit δ_μ den vierten Coefficienten der Substitution $\begin{pmatrix} 0, & +1 \\ -1, & \delta_\mu \end{pmatrix}$, durch welche φ_μ in die nach rechts benachbarte Form $\varphi_{\mu+1}$ übergeht, und endlich mit k_μ den absoluten Werth von δ_μ. Da (nach §. 77) der Coefficient δ_μ seinem Zeichen nach mit ω_μ übereinstimmt, und dem absoluten Werth nach die grösste in dem absoluten Werth von ω_μ enthaltene ganze Zahl ist, und da die Wurzeln $\omega_0, \omega_1, \omega_2 \ldots$ abwechselnd positiv und negativ sind, so ist $(-1)^\mu\, \omega_\mu$ stets positiv, und folglich

$$k_\mu = (-1)^\mu\, \delta_\mu;$$

zwischen den successiven Wurzeln $\omega_\mu, \omega_{\mu+1} \ldots$ bestehen aber folgende Relationen (§. 77):

$$\omega_\mu = \delta_\mu - \frac{1}{\omega_{\mu+1}};\ \omega_{\mu+1} = \delta_{\mu+1} - \frac{1}{\omega_{\mu+2}} \cdots$$

multiplicirt man diese Gleichungen der Reihe nach mit $\pm 1, \mp 1$ u. s. w. der Art, dass die linke Seite stets positiv wird, so erhält man

$$\pm\omega_\mu = k_\mu + \frac{1}{\mp\omega_{\mu+1}};\ \mp\omega_{\mu+1} = k_{\mu+1} + \frac{1}{\pm\omega_{\mu+2}} \cdots$$

und hieraus ergiebt sich für den positiven irrationalen unechten Bruch $(-1)^\mu\ \omega_\mu$ folgender Kettenbruch:

$$(-1)^\mu\ \omega_\mu = k_\mu + \cfrac{1}{k_{\mu+1} + \cfrac{1}{k_{\mu+2} + \cdots}}$$

den wir kürzer durch

$$(k_\mu,\ k_{\mu+1},\ k_{\mu+2} \ldots)$$

bezeichnen wollen. Offenbar ist dieser Kettenbruch periodisch; denn besteht die Periode der reducirten Formen φ aus $2n$ Gliedern, so ist $\delta_{\mu+2n} = \delta_\mu$ und also auch $k_{\mu+2n} = k_\mu$; es wiederholt sich daher die Reihe der Zahlen k immer nach höchstens $2n$ Gliedern von Neuem.

Beispiel 1: Nehmen wir $D = 13$, so haben wir, um die erste Wurzel ω_0 der Form $\varphi_0 = (3,\ 1,\ -4)$ in einen Kettenbruch zu entwickeln, ihre Periode aufzustellen (§. 78):

$$\begin{aligned}
\varphi_0 &= (3,\ 1,\ -4); & \varphi_1 &= (-4,\ 3,\ 1)\\
\varphi_2 &= (1,\ 3,\ -4); & \varphi_3 &= (-4,\ 1,\ 3)\\
\varphi_4 &= (3,\ 2,\ -3); & \varphi_5 &= (-3,\ 1,\ 4)\\
\varphi_6 &= (4,\ 3,\ -1); & \varphi_7 &= (-1,\ 3,\ 4)\\
\varphi_8 &= (4,\ 1,\ -3); & \varphi_9 &= (-3,\ 2,\ 3)
\end{aligned}$$

und hieraus durch die Formel $\delta = -\dfrac{b + b'}{a'}$ die successiven Werthe der Substitutionscoefficienten δ abzuleiten:

$$\begin{aligned}
&\delta_0 = +1,\ \delta_1 = -6,\ \delta_2 = +1,\ \delta_3 = -1,\ \delta_4 = +1,\\
&\delta_5 = -1,\ \delta_6 = +6,\ \delta_7 = -1,\ \delta_8 = +1,\ \delta_9 = -1;
\end{aligned}$$

daraus ergeben sich die absoluten Werthe

$$\begin{aligned}
&k_0 = 1,\ k_1 = 6,\ k_2 = 1,\ k_3 = 1,\ k_4 = 1,\\
&k_5 = 1,\ k_6 = 6,\ k_7 = 1,\ k_8 = 1,\ k_9 = 1.
\end{aligned}$$

Hier zeigt sich die eigenthümliche Erscheinung, dass die Periode des Kettenbruchs nur aus fünf Gliedern besteht, während die Periode der Formen doppelt so viele Glieder enthält; wir werden

später darauf zurückkommen. Die gesuchte Kettenbruch-Entwicklung ergiebt sich hieraus als die folgende:

$$\frac{1+\sqrt{13}}{4} = (1, 6, 1, 1, 1;\ 1, 6, 1, 1, 1; \ldots)$$

Ebenso liefern die beiden andern reducirten Formen derselben Determinante $D = 13$, nämlich

$$\varphi_0 = (2, 3, -2), \quad \varphi_1 = (-2, 3, 2)$$

folgende Werthe

$$\delta_0 = +3, \quad \delta_1 = -3,$$

also

$$k_0 = 3, \qquad k_1 = 3$$

und folglich

$$\frac{3+\sqrt{13}}{2} = (3;\ 3; \ldots);$$

auch hier ist die Periode des Kettenbruchs nur halb so gross wie die der reducirten Formen.

Beispiel 2: Für $D = 19$ giebt die sechsgliedrige Formenperiode

$$\varphi_0 = (3, 2, -5); \quad \varphi_1 = (-5, 3, 2)$$
$$\varphi_2 = (2, 3, -5); \quad \varphi_3 = (-5, 2, 3)$$
$$\varphi_4 = (3, 4, -1); \quad \varphi_5 = (-1, 4, 3)$$

die Zahlen

$$\delta_0 = +1,\ \delta_1 = -3,\ \delta_2 = +1,\ \delta_3 = -2,\ \delta_4 = +8,\ \delta_5 = -2;$$
$$k_0 = 1, \quad k_1 = 3, \quad k_2 = 1, \quad k_3 = 2, \quad k_4 = 8, \quad k_5 = 2;$$

also

$$\frac{2+\sqrt{19}}{5} = (1, 3, 1, 2, 8, 2; \ldots)$$

Beispiel 3: Für $D = 79$ giebt die sechsgliedrige Periode

$$\varphi_0 = (7, 3, -10); \quad \varphi_1 = (-10, 7, 3)$$
$$\varphi_2 = (3, 8, -5); \quad \varphi_3 = (-5, 7, 6)$$
$$\varphi_4 = (6, 5, -9); \quad \varphi_5 = (-9, 4, 7)$$

die Zahlen

$$\delta_0 = +1,\ \delta_1 = -5,\ \delta_2 = +3,\ \delta_3 = -2,\ \delta_4 = +1,\ \delta_5 = -1;$$
$$k_0 = 1,\quad k_1 = 5,\quad k_2 = 3,\quad k_3 = 2,\quad k_4 = 1,\quad k_5 = 1;$$

also entsteht die Entwicklung

$$\frac{3 + \sqrt{79}}{10} = (1,\ 5,\ 3,\ 2,\ 1,\ 1;\ \ldots).$$

Ebenso liefert die viergliedrige Periode

$$\varphi_0 = (1,\ 8,\ -15);\quad \varphi_1 = (-15,\ 7,\ 2)$$
$$\varphi_2 = (2,\ 7,\ -15);\quad \varphi_3 = (-15,\ 8,\ 1)$$

die Zahlen

$$\delta_0 = +1,\ \delta_1 = -7,\ \delta_2 = +1,\ \delta_3 = -16;$$
$$k_0 = 1,\ k_1 = 7,\ k_2 = 1,\ k_3 = 16;$$

also den Kettenbruch

$$\frac{8 + \sqrt{79}}{15} = (1,\ 7,\ 1,\ 16;\ \ldots).$$

Zu gleicher Zeit findet man natürlich auch die Entwicklung der Wurzeln der drei andern Formen

$$-\frac{7 + \sqrt{79}}{2} = -(7,\ 1,\ 16,\ 1;\ \ldots)$$
$$\frac{7 + \sqrt{79}}{15} = (1,\ 16,\ 1,\ 7;\ \ldots)$$
$$-\frac{8 + \sqrt{79}}{1} = -(16,\ 1,\ 7,\ 1;\ \ldots)$$

durch einfache Verschiebung der Periode *).

---

*) Die Form $(1, 0, -D)$ ist der reducirten Form $\varphi_0 = (1, \lambda, \lambda^2 - D)$ äquivalent; die letzte Form der entsprechenden Periode ist offenbar $\varphi_{2n-1} = (\lambda^2 - D, \lambda, 1)$, und hieraus folgt eine Entwicklung von der Form:

$$\frac{1}{\sqrt{D} - \lambda} = (k_0 \ldots k_{n-2},\ k_{n-1},\ k_{n-2} \ldots k_0,\ 2\lambda;\ \ldots).$$

und

$$\sqrt{D} = (\lambda;\ k_0 \ldots k_{n-2},\ k_{n-1},\ k_{n-2} \ldots k_0,\ 2\lambda; \ldots).$$

Ist ferner $D \equiv 1 \pmod{4}$, und λ' die grösste *ungerade* Zahl unterhalb $\sqrt{D}$, so ist die Form $(2, 1, \frac{1}{2}(1 - D))$ der reducirten Form $(2, \lambda', \frac{1}{2}(\lambda'^2 - D))$ äquivalent, und da die letzte Form der entsprechenden Periode nothwendig $(\frac{1}{2}(\lambda'^2 - D), \lambda', 2)$ ist, so ergiebt sich eine ganz ähnliche Entwicklung für $\frac{1}{2}(\sqrt{D} - 1)$.

§. 80.

Es bleibt nun noch die schwierigste Frage zu beantworten übrig, nämlich die, ob zwei reducirte Formen derselben Determinante, welche verschiedenen Perioden angehören, äquivalent sein können oder nicht. Dazu müssen wir eine Digression über die Theorie der Kettenbrüche machen, in welcher wir einige weniger bekannte Sätze über dieselben beweisen wollen.

Ein Kettenbruch $(a, b, c, d \ldots)$, dessen sämmtliche Elemente $a, b, c, d \ldots$ positive ganze Zahlen sind (mit Ausnahme des ersten a, für welches auch der Werth Null gestattet ist), soll im Folgenden ein *regelmässiger* heissen; der Werth eines solchen, endlichen oder unendlichen Kettenbruchs ist bekanntlich stets positiv, und umgekehrt ist bekannt, dass jeder positive Werth stets und nur auf eine einzige Weise in einen regelmässigen Kettenbruch verwandelt werden kann. Sehr wichtig für unsere Zwecke ist nun die Umwandlung eines unregelmässigen unendlichen Kettenbruchs

$$(\alpha, \beta, \gamma \ldots \mu, \nu, p, q, r \ldots u, v \ldots),$$

dessen Elemente ganze Zahlen und zwar von einem bestimmten p ab sämmtlich positive ganze Zahlen sind, in einen regelmässigen. Es wird sich zeigen, dass bei dieser Umwandlung alle Elemente $u, v \ldots$ von einem bestimmten, in endlicher Entfernung liegenden, Element u ab unverändert bleiben, und dass die Differenz zwischen der Anzahl der geänderten und der Anzahl der sie ersetzenden Elemente eine gerade oder ungerade Zahl ist, je nachdem der Werth des ganzen Kettenbruchs positiv oder negativ ist.

Um dies zu beweisen, nehmen wir an, es sei ν das letzte nicht positive Element des Kettenbruchs, und wir setzen ausserdem zunächst voraus, dass ν nicht das erste Element des ganzen Kettenbruchs ist. Wir suchen nun die Unregelmässigkeit des Kettenbruchs von dieser äussersten Stelle ν zu entfernen und um mindestens eine Stelle weiter nach links zu drängen.

Hierzu brauchen wir offenbar nur den unendlichen Kettenbruch $(\mu, \nu, p, q \ldots)$ zu betrachten, den wir auch in endlicher Form (μ, ν, p') oder (μ, ν, p, q') oder (μ, ν, p, q, r') u. s. w. schreiben können, wenn wir die unendlichen regelmässigen Kettenbrüche

$$(p, q, r, s \ldots), \quad (q, r, s \ldots), \quad (r, s \ldots) \text{ u. s. w.}$$

zur Abkürzung mit p', q', r' u. s. w. bezeichnen. Wir haben nun folgende Fälle zu unterscheiden.

1) Ist $\nu = 0$, so ist

$$(\mu, 0, p') = \mu + \cfrac{1}{0 + \cfrac{1}{p'}} = \mu + p' = \mu + p + \frac{1}{q'}$$

oder also

$$(\mu, 0, p, q') = (\mu + p, q');$$

es ist also die Unregelmässigkeit von der Stelle $\nu = 0$ um mindestens eine Stelle nach links gedrängt, und zugleich ist an Stelle der abgeänderten drei Elemente μ, 0, p das einzige Element $\mu + p$ getreten.

2) Ist ν negativ $= -n$, und $n > 1$, so erhält man mit Benutzung der Identität

$$(g, -h) = g - \frac{1}{h} = g - 1 + \cfrac{1}{1 + \cfrac{1}{h-1}} = (g-1, 1, h-1)$$

folgende successive Umformung:

$$(\mu, -n, p') = \left(\mu, -n + \frac{1}{p'}\right) = \left(\mu - 1, 1, n - 1 - \frac{1}{p'}\right)$$
$$= (\mu - 1, 1, n - 1, -p')$$

und hieraus durch nochmalige Anwendung derselben Identität:

$$(\mu, -n, p, q') = (\mu - 1, 1, n - 2, 1, p' - 1)$$
$$= (\mu - 1, 1, n - 2, 1, p - 1, q').$$

An Stelle der drei abgeänderten Elemente μ, $-n$, p sind die fünf Elemente $\mu - 1$, 1, $n - 2$, 1, $p - 1$ getreten, und von diesen ist höchstens das erste negativ. Sollte ferner $n - 2$ oder $p - 1$, oder sollten beide Zahlen $= 0$ sein, so wird man durch einmalige oder zweimalige Anwendung der unter 1) aufgestellten Regel alle Elemente, mit Ausnahme des ersten, in positive verwandeln; auch dann wird der Unterschied zwischen der Anzahl der abgeänderten und der Anzahl der dieselben ersetzenden Elemente eine gerade Zahl bleiben, und die Unregelmässigkeit ist mindestens um eine Stelle nach links verschoben.

3) Ist $\nu = -1$, so ist die eben angegebene Regel nicht anwendbar; wenn gleichzeitig $p > 1$, so findet man

$$(\mu, -1, p') = \mu + \cfrac{1}{-1 + \cfrac{1}{p'}} = \mu - 2 + \cfrac{1}{1 + \cfrac{1}{p' - 2}}$$

also auch

$$(\mu, -1, p, q') = (\mu - 2, 1, p - 2, q');$$

sollte $p = 2$ sein, so hat man wieder nach der unter 1) aufgestellten Regel zu verfahren. Ist aber $p = 1$, so hilft diese Formel Nichts; dann ist aber

$$(\mu, -1, 1, q') = \mu + \cfrac{1}{-1 + \cfrac{1}{1 + \cfrac{1}{q'}}} = \mu - 1 - q'$$

und folglich

$$(\mu, -1, 1, q, r, s') = (\mu - 2 - q, 1, r - 1, s');$$

und sollte $r = 1$ sein, so würde man wie in 1) verfahren.

Auf diese Weise ist in allen Fällen ohne Ausnahme die Unregelmässigkeit des Kettenbruchs von der Stelle ν um mindestens eine Stelle weiter nach links gedrängt, und zugleich ist der Unterschied zwischen der Anzahl der abgeänderten und der Anzahl der sie ersetzenden Elemente jedes Mal eine gerade Zahl. Durch successive Anwendung desselben Verfahrens wird man daher den ursprünglich gegebenen Kettenbruch

$$(\alpha, \beta, \gamma \ldots \mu, \nu, p, q, r \ldots t, u, v \ldots)$$

in einen andern

$$(\alpha', b, c \ldots k, l, u, v \ldots)$$

umformen können, in welchem alle auf das erste folgenden Elemente $b, c \ldots$ positive ganze Zahlen sind, welche von einer in endlicher Entfernung liegenden Stelle u an mit den Elementen des gegebenen Kettenbruchs übereinstimmen; und zwar wird der Unterschied zwischen der Anzahl der abgeänderten Elemente

$$\alpha, \beta, \gamma \ldots \mu, \nu, p, q, r \ldots t$$

und der Anzahl der sie ersetzenden Elemente

$$\alpha', b, c \ldots k, l$$

eine gerade Zahl sein, weil dasselbe bei jedem einzelnen Act der gesammten Umformung Statt findet.

Ist nun α' positiv oder $= 0$, so ist die Umformung vollendet und der Werth des Kettenbruchs ist positiv; ist dagegen α' negativ $= - a$, so ist der Kettenbruch negativ, und zwar

$$= - (a - 1, 1, b - 1, c \ldots)$$

oder, wenn $b = 1$ sein sollte,

$$= - (a - 1, c + 1, d \ldots).$$

Bei diesem letzten Act ist die Anzahl der abgeänderten Elemente um eine Einheit kleiner oder grösser als die Anzahl der sie ersetzenden Elemente; und hiermit ist der letzte Punct unserer obigen Behauptung nachgewiesen.

§. 81.

Wir bedürfen zweitens für die Untersuchung der Aequivalenz zweier Formen noch des folgenden Satzes:

Sind $\alpha, \beta, \gamma, \delta$ vier ganze Zahlen, welche der Bedingung

$$\alpha\delta - \beta\gamma = 1$$

genügen, und deren erste α von Null verschieden ist; findet ferner zwischen zwei Grössen ω und Ω die Relation

$$\omega = \frac{\gamma + \delta\Omega}{\alpha + \beta\Omega}$$

Statt; so kann man stets

$$\omega = (\lambda, m, n \ldots r, \sigma, \Omega)$$

setzen, wo die Anzahl der positiven ganzen Zahlen $m, n \ldots r$ eine gerade ist, λ und σ aber auch Null oder negative ganze Zahlen sein können.

Um diesen Satz zu beweisen, können wir, ohne die Allgemeinheit zu beeinträchtigen, annehmen, dass die von Null verschiedene ganze Zahl α positiv ist; denn sollte α negativ sein, so verwandele man die Zeichen aller vier Zahlen $\alpha, \beta, \gamma, \delta$ in die entgegen-

gesetzten, so bleibt die zwischen ihnen, und ebenso die zwischen ω und Ω bestehende Relation ungeändert. Ist nun zunächst $\alpha = 1$, also $\delta = \beta\gamma + 1$, so ist unmittelbar

$$\omega = \frac{\gamma + (\beta\gamma + 1)\Omega}{1 + \beta\Omega} = \gamma + \frac{\Omega}{1 + \beta\Omega} = (\gamma, \beta, \Omega),$$

also ist in diesem Fall unser Satz richtig. Ist aber $\alpha > 1$, so entwickle man den Bruch $\frac{\gamma}{\alpha}$ in den Kettenbruch $(\lambda, m, n \ldots r)$, dessen Elemente sämmtlich positive ganze Zahlen sind, mit Ausnahme des ersten λ, welches positiv, Null oder negativ sein wird, je nachdem γ positiv und grösser als α, oder positiv und kleiner als α, oder endlich negativ ist.

Wir können ferner voraussetzen, dass die Anzahl der positiven Elemente $m, n \ldots r$ gerade ist; denn da bei der gewöhnlichen Methode, einen Bruch $\frac{\gamma}{\alpha}$ in einen Kettenbruch zu verwandeln, das letzte Element r mindestens $= 2$ ist, so könnte man, wenn die Anzahl der Elemente $m, n \ldots r$ ungerade sein sollte, das letzte Element r in den Kettenbruch $r - 1 + \frac{1}{1}$ verwandeln und also statt des obigen Kettenbruchs den folgenden $(\lambda, m, n \ldots r - 1, 1)$ nehmen, in welchem die Anzahl der positiven Elemente $m, n \ldots r - 1, 1$ nun gerade ist. Bildet man nun nach der früher (§. 23) angegebenen Methode die sogenannten Näherungsbrüche,

$$\frac{[\lambda]}{1}, \frac{[\lambda, m]}{[m]}, \frac{[\lambda. m, n]}{[m, n]} \ldots \frac{[\lambda, m, n \ldots q, r]}{[m, n \ldots q, r]},$$

so erkennt man leicht, dass ihre Nenner sämmtlich positiv sind. Damals haben wir auch bewiesen, dass diese Brüche irreductibel sind, und da der letzte der obigen Brüche dem in Folge der Relation $\alpha\delta - \beta\gamma = 1$ ebenfalls irreductibeln Bruche $\frac{\gamma}{\alpha}$ gleich, und α positiv ist, so muss

$$\alpha = [m, n \ldots q, r], \quad \gamma = [\lambda, m, n \ldots q, r]$$

sein, weil ein Bruch nur auf eine einzige Weise in die irreductibele Form mit positivem Nenner gebracht werden kann. Da ferner die Anzahl der Elemente $\lambda, m, n \ldots q, r$ ungerade ist, so folgt aus

der damals aufgestellten Formel [§. 23, (9)], dass

$$[m, n \ldots q]\,[\lambda, m, n \ldots q, r] - [m, n \ldots q, r]\,[\lambda, m, n \ldots q] = -1$$

oder also

$$\alpha\,[\lambda, m, n \ldots q] - [m, n \ldots q]\,\gamma = 1$$

ist; vergleicht man dies mit der Relation $\alpha\delta - \beta\gamma = 1$, so ergiebt sich (ähnlich wie im §. 59), dass man

$$\delta = [\lambda, m, n \ldots q] + \gamma\sigma$$
$$\beta = [m, n \ldots q] + \alpha\sigma$$

d. h.

$$\delta = [\lambda, m, n \ldots q, r, \sigma]$$

$$\beta = [m, n \ldots q, r, \sigma]$$

also

$$\frac{\delta}{\beta} = (\lambda, m, n \ldots q, r, \sigma)$$

setzen kann. Nach demselben Bildungsgesetz ist nun

$$\gamma + \delta\Omega = [\lambda, m, n \ldots r, \sigma, \Omega]$$
$$\alpha + \beta\Omega = [m, n \ldots r, \sigma, \Omega]$$

und folglich, wie zu beweisen war,

$$\omega = (\lambda, m, n \ldots r, \sigma, \Omega).$$

§. 82.

Nachdem auch dieser zweite Punct aus der Theorie der Kettenbrüche behandelt ist, schreiten wir zur definitiven Entscheidung der Frage, ob zwei verschiedene Perioden von reducirten Formen einer positiven Determinante äquivalente Formen enthalten können. Es seien daher (a, b, c) und (A, B, C) zwei reducirte (eigentlich) äquivalente Formen; da alle Formen einer und derselben Periode einander stets äquivalent sind, so können wir annehmen, dass die ersten Coefficienten a, A und folglich auch die ersten Wurzeln dieser beiden Formen positiv sind, weil im entgegengesetzten Fall die unmittelbar benachbarten Formen diese

Eigenschaft besitzen würden. Bezeichnen wir (a, b, c) mit φ_0 und (A, B, C) mit Φ_0, und bilden wir für jede dieser beiden Formen (nach §. 78) die sie enthaltende Periode, so erhalten wir dadurch für die ersten Wurzeln ω_0, Ω_0 dieser beiden Formen die regelmässigen Kettenbrüche

$$\omega_0 = (k_0, \ k_1, \ k_2 \ \ldots),$$
$$\Omega_0 = (K_0, K_1, K_2 \ldots).$$

Ist nun $\begin{pmatrix}\alpha, \beta \\ \gamma, \delta\end{pmatrix}$ eine Substitution, durch welche φ_0 in Φ_0 übergeht, so besteht zwischen den ersten Wurzeln ω_0, Ω_0 die Relation

$$\omega_0 = \frac{\gamma + \delta\Omega_0}{\alpha + \beta\Omega_0}$$

und ausserdem ist

$$\alpha\delta - \beta\gamma = 1.$$

Da ferner α nicht $= 0$ sein kann, weil sonst $A = c$, also A negativ wäre, so kann man nach dem so eben bewiesenen Satze

$$\omega_0 = (\lambda, m, n \ldots r, \sigma, \Omega_0)$$

und also auch

$$\omega_0 = (\lambda, m, n \ldots r, \sigma, K_0, K_1, K_2 \ldots)$$

setzen, und in diesem unendlichen Kettenbruch, welcher wenigstens von der Stelle K_0 ab keine Unregelmässigkeit enthält, ist die Anzahl der Elemente $\lambda, m, n \ldots r, \sigma$ eine gerade $= 2g$. Ist σ positiv, so ist, da $\omega_0 > 1$ ist, auch λ positiv, also der Bruch regelmässig. Ist aber $\sigma = 0$ oder negativ, so forme man den Kettenbruch nach den obigen Regeln (§. 80) in einen regelmässigen um; nimmt man μ hinreichend gross, so werden die Elemente K_μ, $K_{\mu+1} \ldots$ bei dieser Umformung ungeändert bleiben, und die Anzahl ν der Elemente, welche an die Stelle der vorhergehenden $(2g + \mu)$ Elemente

$$\lambda, m, n \ldots r, \sigma, K_0 \ldots K_{\mu-1}$$

treten, wird $\equiv \mu \pmod{2}$ sein (nach §. 80), da der Werth des ganzen Kettenbruchs *positiv* ist. Da nun ω_0 nur auf eine einzige Weise als ein regelmässiger Kettenbruch dargestellt werden kann, so müssen die Zahlen

$$K_\mu, \ K_{\mu+1}, \ K_{\mu+2} \ldots\ldots$$

resp. mit den Zahlen

$$k_\nu, \ k_{\nu+1}, \ k_{\nu+2} \ldots\ldots$$

identisch sein. Ist daher $\mu + h$ ein Multiplum von der Anzahl der Formen, welche die Periode der Form Φ_0 bilden, und also eine gerade Zahl, so ist auch $\nu + h$ eine gerade Zahl $= 2m$, und die Zahlen

$$K_{\mu+h}, \ K_{\mu+h+1}, \ K_{\mu+h+2} \ldots$$

stimmen mit den Zahlen

$$K_0, \ K_1, \ K_2 \ldots,$$

und diese folglich mit den Zahlen

$$k_{2m}, \ k_{2m+1}, \ k_{2m+2} \ldots$$

überein. Hieraus folgt unmittelbar

$$\Omega_0 = (k_{2m}, \ k_{2m+1} \ldots) = \omega_{2m};$$

und da durch ihre erste Wurzel auch stets die Form vollständig charakterisirt ist, so schliessen wir hieraus, dass die Form Φ_0 mit der Form φ_{2m} identisch sein muss, dass also Φ_0 sich in der aus φ_0 entwickelten Periode befinden muss. Wir haben so folgenden *Hauptsatz* gewonnen:

Zwei äquivalente reducirte Formen von positiver Determinante gehören einer und derselben Periode an; zwei reducirte Formen können nicht äquivalent sein, wenn sie verschiedenen Perioden angehören.

Mit Hülfe dieses Satzes ergiebt sich nun eine Methode, um zu prüfen, ob zwei gegebene Formen von gleicher positiver Determinante äquivalent sind oder nicht. Man suche (nach §. 76) zu jeder der beiden Formen eine ihr äquivalente reducirte Form; je nachdem die so gefundenen reducirten Formen derselben oder verschiedenen Perioden angehören, sind die gegebenen Formen äquivalent, oder nicht äquivalent. Im erstern Fall ergiebt sich offenbar zugleich eine Substitution, durch welche die eine Form in die andere übergeht.

Beispiel: Die beiden gegebenen Formen seien (713, 60, 5) und (62, 95, 145), welche dieselbe Determinante $D = 35$ haben,

Die erste geht durch die Substitution $\begin{pmatrix} 0, & +1 \\ -1, & -13 \end{pmatrix}$ in die reducirte Form (5, 5, — 2), die zweite durch die Substitution $\begin{pmatrix} -3, & +10 \\ +2, & -7 \end{pmatrix}$ in die reducirte Form (— 2, 5, 5) über. Diese beiden reducirten Formen gehören aber derselben zweigliedrigen Periode

$$(5, 5, -2), \quad (-2, 5, 5)$$

an, und zwar geht die erstere durch die Substitution $\begin{pmatrix} 0, & 1 \\ -1, & 5 \end{pmatrix}$ in die letztere über. Mithin sind die beiden gegebenen Formen (713, 60, 5) und (62, 95, 145) äquivalent, und da $\begin{pmatrix} -7, & -10 \\ -2, & -3 \end{pmatrix}$ die inverse Substitution von $\begin{pmatrix} -3, & +10 \\ +2, & -7 \end{pmatrix}$ ist, so geht die erstere dieser beiden Formen durch die Substitution

$$\begin{pmatrix} 0, & +1 \\ -1, & -13 \end{pmatrix}\begin{pmatrix} 0, & 1 \\ -1, & 5 \end{pmatrix}\begin{pmatrix} -7, & -10 \\ -2, & -3 \end{pmatrix} = \begin{pmatrix} -3, & -5 \\ +41, & +68 \end{pmatrix}$$

in die letztere über.

§. 83.

Durch unsere letzten Untersuchungen ist das erste der beiden in §. 59 aufgestellten Hauptprobleme auch für Formen von positiver Determinante gelöst; das zweite haben wir, indem wir uns auf ursprüngliche Formen beschränkten, in §. 61 auf die Auflösung der unbestimmten Gleichung

$$t^2 - Du^2 = \sigma^2$$

zurückgeführt, und es bleibt daher, um in der Theorie der Formen von positiver Determinante zu demselben Abschluss zu kommen, wie früher für negative Determinanten, nur noch übrig, diese Gleichung für jeden positiven (nicht quadratischen) Werth der Determinante D vollständig aufzulösen. *Fermat* hat diese Gleichung den Mathematikern zuerst vorgelegt, worauf ihre Lösung von dem Engländer *Pell* angegeben wurde; allein obwohl seine Methode die Lösung in jedem Fall wirklich giebt, so lag doch in ihr nicht der Nachweis, dass sie immer zum Ziele führen muss und dass die Gleichung ausser der evidenten Auflösung $t = \pm \sigma$,

$u = 0$ noch andere Auflösungen besitzt. Diese Lücke ist erst von *Lagrange* ausgefüllt, und hierin besteht wohl eine der bedeutendsten Leistungen des grossen Mathematikers auf dem Gebiete der Zahlentheorie, da die von ihm zu diesem Zweck eingeführten Principien in hohem Grade der Verallgemeinerung fähig und deshalb auch auf ähnliche höhere Probleme anwendbar sind*).

Wir schlagen hier einen ganz andern Weg ein, der sich den zunächst vorangehenden Untersuchungen unmittelbar anschliesst. Der Zusammenhang zwischen der obigen unbestimmten Gleichung und dem zweiten Hauptproblem in der Theorie der Aequivalenz war folgender. Ist (a, b, c) eine ursprüngliche Form der σten Art von der Determinante D, und ist $\begin{pmatrix}\alpha, & \beta \\ \gamma, & \delta\end{pmatrix}$ irgend eine eigentliche Substitution, durch welche (a, b, c) in sich selbst übergeht so ist stets

$$\alpha = \frac{t - bu}{\sigma},\ \ \beta = -\frac{cu}{\sigma},\ \ \gamma = \frac{au}{\sigma},\ \ \delta = \frac{t + bu}{\sigma},$$

wo t, u zwei der Gleichung

$$t^2 - Du^2 = \sigma^2$$

genügende ganze Zahlen bedeuten; und umgekehrt, jeder Auflösung t, u der unbestimmten Gleichung entspricht durch die vorstehenden Formeln eine Substitution $\begin{pmatrix}\alpha, & \beta \\ \gamma, & \delta\end{pmatrix}$, durch welche die Form (a, b, c) in sich selbst übergeht. Wir haben nun durch die letzten Untersuchungen, wie sich gleich zeigen wird, ein Mittel gewonnen, alle Transformationen $\begin{pmatrix}\alpha, & \beta \\ \gamma, & \delta\end{pmatrix}$ einer reducirten Form von positiver Determinante D in sich selbst direct zu finden, und folglich können wir hieraus auch alle Auflösungen t, u der unbestimmten Gleichung ableiten. Wir schicken der Ausführung dieser Untersuchung noch eine Bemerkung über die Perioden der reducirten Formen voraus.

Wir wissen, dass die Reihe der positiven Zahlen k, welche die Elemente des Kettenbruchs bilden, in den die erste Wurzel

*) Siehe die Supplemente VIII.

ω_0 einer reducirten Form φ_0 entwickelt wird, eine gerade Anzahl von Gliedern

$$k_0, \; k_1 \ldots k_{2n-1}$$

enthält, nach welchen dieselben Glieder periodisch wiederkehren; und zwar ist diese Anzahl $2n$ die der reducirten Formen, welche mit φ_0 in einer Periode enthalten sind. Wir haben aber oben (§. 79) an einzelnen Beispielen gesehen, dass die Zahlen k aus kleinern Perioden bestehen können; wir fanden z. B. aus der zehngliedrigen Formenperiode der Determinante $D = 13$ folgende Zahlen:

$$\delta_0 = +1, \; \delta_1 = -6, \; \delta_2 = +1, \; \delta_3 = -1, \; \delta_4 = +1;$$
$$\delta_5 = -1, \; \delta_6 = +6, \; \delta_7 = -1, \; \delta_8 = +1, \; \delta_9 = -1;$$

und also

$$k_0 = 1, \; k_1 = 6, \; k_2 = 1, \; k_3 = 1, \; k_4 = 1;$$

und hierauf wiederholt sich schon dieselbe Reihe

$$k_5 = 1, \; k_6 = 6, \; k_7 = 1, \; k_8 = 1, \; k_9 = 1.$$

Es ist nun wichtig zu untersuchen, wann dies eintreten kann. Es sei daher $2n$ die Gliederanzahl der Formenperiode und m die Gliederanzahl irgend einer Periode in der Reihe der Zahlen k. Dann ist, indem wir die frühern Bezeichnungen für die Formen und ihre ersten Wurzeln beibehalten, wenn m gerade ist,

$$\omega_m = (k_m, \; k_{m+1} \ldots) = (k_0, \; k_1 \ldots)$$

und folglich $\omega_m = \omega_0$, und also auch φ_m identisch mit φ_0 und daher nothwendig m ein Multiplum von $2n$; es existirt also jedenfalls keine kleinere Periode von gerader Gliederanzahl als die der ganzen Formenperiode entsprechende. Ist dagegen m ungerade, so ist $2m$ ebenfalls die Gliederanzahl einer Periode in der Reihe der Zahlen k, und folglich ist nach dem eben Bewiesenen $2m$ ein Multiplum von $2n$, also m mindestens $= n$; der Fall, dass die Periode der Zahlen k kürzer ist als die aus $2n$ Gliedern bestehende Periode der Formen, kann also nur dann eintreten, wenn n eine ungerade Zahl ist, indem dann, wie wir ja auch an dem obigen Beispiel sehen, die Periode der Zahlen k aus n Gliedern bestehen kann; es ist dann $\omega_n = -\omega_0$, und also $c_n = -c_0$, $b_n = b_0$,

$a_n = -a$. Doch muss man sich hüten zu glauben, dass diese Erscheinung jedesmal wirklich eintreten *muss*, wenn n ungerade ist; denn wir haben nur gezeigt, dass sie in diesem Fall allein eintreten *kann*. Für $D = 19$ z. B. sind die beiden Formenperioden sechsgliedrig (§. 79), also ist $n = 3$; aber die Perioden der Zahlen k sind nicht dreigliedrig, sondern sechsgliedrig.

Um nun die unbestimmte Gleichung $t^2 - Du^2 = \sigma^2$ zu lösen, in welcher D eine beliebige nicht quadratische positive Zahl, und $\sigma = 1$ oder (wenn $D \equiv 1 \pmod{4}$ ist) auch $= 2$ sein kann, nehmen wir eine beliebige *ursprüngliche reducirte* Form (a, b, c) der Determinante D und von der σten Art. Dass eine solche stets existirt, leuchtet daraus ein, dass in allen Fällen die Form $(1, 0, -D)$ ursprünglich und von der ersten Art, und im Fall $D \equiv 1 \pmod{4}$ die Form $(2, 1, -\frac{1}{2}(D-1))$ ursprünglich und von der zweiten Art ist; sucht man nun zu diesen beiden Formen die ihnen äquivalenten reducirten Formen, so sind die letztern nothwendig ebenfalls ursprünglich und auch von derselben Art wie jene. Wir nehmen ferner, was stets gestattet ist, a positiv, und folglich c negativ an; dann ist die erste Wurzel ω dieser Form positiv, und folglich

$$\omega = (k_0, \ k_1 \ldots k_{2hn-2}, \ k_{2hn-1}, \ \omega),$$

wo $2n$ die Gliederanzahl der Formenperiode, und h eine beliebige positive ganze Zahl ist. Setzt man nun

$$\frac{\gamma}{\alpha} = (k_0, \ k_1 \ldots k_{2hn-2}); \quad \frac{\delta}{\beta} = (k_0, \ k_1 \ldots k_{2hn-1})$$

d. h. (nach §. 23)

$$\alpha = [k_1 \ldots k_{2hn-2}], \quad \beta = [k_1 \ldots k_{2hn-2}, \ k_{2hn-1}],$$
$$\gamma = [k_0, \ k_1 \ldots k_{2hn-2}], \quad \delta = [k_0, \ k_1 \ldots k_{2hn-2}, \ k_{2hn-1}],$$

so ist nach den schon öfter benutzten Sätzen $\alpha\delta - \beta\gamma = 1$ und

$$\alpha + \beta\omega = [k_1 \ldots k_{2hn-2}, \ k_{2hn-1}, \ \omega]$$
$$\gamma + \delta\omega = [k_0, \ k_1 \ldots k_{2hn-2}, \ k_{2hn-1}, \ \omega]$$

und folglich

$$\frac{\gamma + \delta\omega}{\alpha + \beta\omega} = (k_0, \ k_1 \ldots k_{2hn-2}, k_{2hn-1}, \omega) = \omega.$$

Durch die Substitution $\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}$ geht nun die Form (a, b, c) in eine äquivalente Form über, deren erste Wurzel ω' mit ω in der Beziehung

$$\omega = \frac{\gamma + \delta\omega'}{\alpha + \beta\omega'}$$

steht, woraus unmittelbar folgt, dass $\omega' = \omega$ ist; und da eine Form durch ihre erste Wurzel vollständig bestimmt ist, so ergiebt sich, dass die Form (a, b, c) durch die Substitution $\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}$ in sich selbst übergeht.

Setzt man daher für h der Reihe nach alle positiven ganzen Zahlen $1, 2, 3 \ldots$, so erhält man durch die Zähler und Nenner der Näherungsbrüche vom Range $2hn-1$ und $2hn$ jedesmal eine entsprechende Transformation $\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}$ der Form (a, b, c) in sich selbst (wenn $n = 1$ ist und $h = 1$ genommen wird, hat man $\alpha = 1$, $\beta = k_1$, $\gamma = k_0$, $\delta = k_0 k_1 + 1$ zu setzen); die vier Coefficienten $\alpha, \beta, \gamma, \delta$ sind immer positiv, und da ausserdem mit wachsendem h auch nothwendig die Zähler und Nenner der Näherungsbrüche beständig wachsen, so entsprechen zwei verschiedenen Werthen von h auch zwei verschiedene Substitutionen $\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}$.

Umgekehrt wollen wir nun zeigen, dass man auf diese Weise alle die Transformationen $\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}$ der Form (a, b, c) in sich selbst erhält, in denen die vier Coefficienten $\alpha, \beta, \gamma, \delta$ sämmtlich positiv sind. Denn es sei $\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}$ eine solche Substitution, so ist

$$\alpha\delta - \beta\gamma = 1 \quad \text{und} \quad \omega = \frac{\gamma + \delta\omega}{\alpha + \beta\omega},$$

also auch

$$\beta\omega^2 + (\alpha - \delta)\,\omega - \gamma = 0,$$

und zwar müssen dieser quadratischen Gleichung beide Wurzeln der Gleichung genügen. Da nun die eine zwischen 1 und $+\infty$, die andere zwischen -1 und 0 liegt, so muss die linke Seite dieser Gleichung für $\omega = 1$ negativ, für $\omega = -1$ positiv ausfallen; hieraus folgt, dass

$$\gamma + \delta > \alpha + \beta, \quad \beta + \delta > \alpha + \gamma$$

ist, wo die Ungleichheitszeichen die Gleichheit ausschliessen. Da wir beweisen wollen, dass $\frac{\gamma}{\alpha}$ und $\frac{\delta}{\beta}$ zwei auf einander folgende Näherungsbrüche eines regelmässigen Kettenbruchs $(k_0, k_1 \ldots)$ sind, so haben wir vor allem zu zeigen, dass $\gamma \geqq \alpha$ und $\delta > \gamma$ ist, dies ergiebt sich in der That aus den vorstehenden Ungleichungen. Wäre nämlich $\delta \leqq \gamma$, so würde aus der zweiten Ungleichung folgen, dass $\alpha < \beta$ und also auch $\alpha\delta < \beta\gamma$ sein müsste, während doch $\alpha\delta = \beta\gamma + 1$ ist; also ist gewiss $\delta > \gamma$. Wäre ferner $\gamma < \alpha$, also $\alpha = \gamma + \varrho$, wo ϱ eine positive ganze Zahl bedeutet, so würde aus der ersten Ungleichheit folgen, dass $\delta > \beta + \varrho$, also auch

$$\alpha\delta - \beta\gamma > (\beta + \gamma)\,\varrho + \varrho^2$$

wäre; dies ist aber wieder unmöglich, da die linke Seite $= 1$, die rechte aber mindestens $= 3$ ist, weil β, γ, ϱ positive ganze Zahlen bedeuten; also ist in der That $\gamma \geqq \alpha$.

Hieraus folgt nun weiter, dass man

$$\frac{\gamma}{\alpha} = (l, m \ldots q, r)$$

setzen kann, wo die Elemente $l, m \ldots q, r$ sämmtlich positiv sind, und zwar kann man es so einrichten, dass ihre Anzahl ungerade ist, weil man eventuell wieder r in $r - 1 + \frac{1}{1}$ auflösen kann. Nehmen wir ferner zunächst an, dass $\alpha > 1$ ist, so ist auch $\gamma > \alpha$ und γ nicht theilbar durch α, und folglich enthält der Kettenbruch mindestens drei Elemente. Bilden wir daher den unmittelbar vorausgehenden Näherungsbruch

$$\frac{\varphi}{f} = (l, m \ldots q),$$

so folgt aus $\alpha\varphi - f\gamma = 1$ und $\alpha\delta - \beta\gamma = 1$, dass man wieder $\beta = f + \alpha s$, $\delta = \varphi + \gamma s$ setzen kann, und hierin wird s eine positive ganze Zahl sein. Wäre nämlich $s = 0$, so wäre $\delta = \varphi$, und da φ gewiss $< \gamma$ ist, so wäre $\delta < \gamma$, während doch $\delta > \gamma$ ist; wäre ferner s negativ, so wäre auch δ negativ, gegen unsere

Voraussetzung, dass $\alpha, \beta, \gamma, \delta$ positive ganze Zahlen sind. Es ist daher

$$\frac{\delta}{\beta} = (l, m \ldots q, r, s)$$

und folglich, ähnlich wie früher,

$$\omega = \frac{\gamma + \delta\omega}{\alpha + \beta\omega} = (l, m \ldots q, r, s, \omega),$$

wo nun die Anzahl der positiven Elemente $l, m \ldots q, r, s$ gerade ist. In dem bisher ausgeschlossenen Fall $\alpha = 1$ erhält man ein ganz ähnliches Resultat, denn dann ist

$$\omega = \frac{\gamma + (\beta\gamma + 1)\,\omega}{1 + \beta\omega} = (\gamma, \beta, \omega).$$

Wir erhalten daher für ω stets einen regelmässigen unendlichen Kettenbruch

$$\omega = (l, m \ldots q, r, s;\ l, m \ldots)$$

in welchem die Anzahl der Glieder $l, m \ldots q, r, s$ eine gerade ist. Da nun ein Werth ω nur auf eine einzige Weise in einen regelmässigen Kettenbruch entwickelt werden kann, so müssen die Zahlen $l, m \ldots$ der Reihe nach mit den Zahlen $k_0, k_1 \ldots$ übereinstimmen; und da wir uns oben überzeugt haben, dass jede Periode der Zahlen k, deren Gliederanzahl gerade ist, entweder mit der Reihe der den sämmtlichen $2n$ Formen entsprechenden Zahlen k identisch ist oder aus einer mehrmaligen Wiederholung dieser kleinsten Periode von gerader Gliederanzahl besteht, so ist also $r = k_{2hn-2}$, $s = k_{2hn-1}$, wo h irgend eine positive ganze Zahl bezeichnet, und folglich

$$\frac{\gamma}{\alpha} = (k_0, k_1 \ldots k_{2hn-2})$$

$$\frac{\delta}{\beta} = (k_0, k_1 \ldots k_{2hn-2}, k_{2hn-1})$$

was zu beweisen war.

Nachdem wir gezeigt haben, wie wir alle aus vier positiven Coefficienten bestehenden Transformationen der reducirten Form (a, b, c) in sich selbst finden können, deren erster Coefficient a

positiv ist, brauchen wir nur noch einen Blick auf die obigen Formeln

$$\alpha = \frac{t - bu}{\sigma},\ \beta = -\frac{cu}{\sigma},\ \gamma = \frac{au}{\sigma},\ \delta = \frac{t + bu}{\sigma}$$

zu werfen, um sogleich zu erkennen, dass die hieraus resultirenden Auflösungen t, u der unbestimmten Gleichung stets aus zwei positiven Zahlen t, u bestehen. Denn da der letzte Coefficient c der reducirten Form (a, b, c) negativ ist, so folgt, dass $u = -\frac{\beta\sigma}{c}$ positiv ist; da ferner, wie wir gesehen haben, $\delta > \gamma$ und $\gamma \geqq \alpha$, also $\delta > \alpha$ ist, so ergiebt sich, dass auch t positiv ist. Das Umgekehrte ist ebenfalls richtig; sind t, u zwei positive der unbestimmten Gleichung genügende Zahlen, so besteht die aus denselben abgeleitete Substitution $\begin{pmatrix}\alpha, & \beta \\ \gamma, & \delta\end{pmatrix}$ aus vier positiven Zahlen; denn da die Form (a, b, c) reducirt, also b positiv und der Annahme nach a positiv, also c negativ ist, so sind zunächst β, γ, δ positiv; endlich ist $t^2 - b^2u^2 = \sigma^2 - acu^2 > 1$ und positiv, folglich hat $t - bu$, also auch α, dasselbe Zeichen wie $t + bu$, nämlich das positive.

§. 84.

Wir können daher behaupten, dass alle aus zwei positiven Zahlen t, u bestehenden Auflösungen — und auf diese kommt es uns zunächst allein an — durch die Kettenbruchentwicklung der Wurzel ω der Form (a, b, c) gefunden werden, und zwar jede nur ein einziges Mal. Aus dem Anblick der unbestimmten Gleichung $t^2 - Du^2 = \sigma^2$ geht aber hervor, dass die zusammengehörigen positiven Werthe t, u gleichzeitig wachsen und gleichzeitig abnehmen; dasselbe folgt auch aus der Natur der Zähler und Nenner der Näherungsbrüche; u und folglich auch t wird gleichzeitig mit γ, also auch mit der von uns mit h bezeichneten Zahl wachsen; nehmen wir $h = 1$, so wird die entsprechende Auflösung, die wir mit T, U bezeichnen wollen, aus den kleinsten Zahlen bestehen, d. h. T wird die kleinste aller Zahlen t, und gleichzeitig

wird U die kleinste aller Zahlen u sein (die Auflösung $t = \sigma$, $u = 0$ gehört natürlich nicht zu den positiven Auflösungen). Diese kleinste Auflösung T, U findet man daher sehr leicht durch Entwicklung einer Periode von reducirten Formen.

Beispiel 1: Nimmt man für die Determinante $D = 79$ die reducirte Form (7, 3, — 10), welche natürlich von der ersten Art ist, so erhält man (§. 79)

$$k_0 = 1,\ k_1 = 5,\ k_2 = 3,\ k_3 = 2,\ k_4 = 1,\ k_5 = 1;$$

die successiven Näherungsbrüche sind folgende:

$$\frac{1}{1},\ \frac{6}{5},\ \frac{19}{16},\ \frac{44}{37},\ \frac{63}{53},\ \frac{107}{90};$$

aus den beiden letzten ergiebt sich daher die Substitution $\begin{pmatrix}53, & 90\\ 63, & 107\end{pmatrix}$; will man nur die kleinste Auflösung der Gleichung $t^2 - Du^2 = \sigma^2$, so braucht man nur die Nenner der Näherungsbrüche bis $\beta = 90$, oder die Zähler derselben bis $\gamma = 63$ zu bilden, so findet man durch die Formeln $\beta = -\frac{cu}{\sigma}$ oder $\gamma = \frac{au}{\sigma}$ die kleinste der Zahlen u, nämlich $U = 9$, und hieraus das zugehörige $T = \sqrt{(\sigma^2 + DU^2)} = 80$. Statt dessen findet man auch T durch die Formel $\frac{1}{2}\sigma(\alpha + \delta)$, wenn man Zähler und Nenner der Näherungsbrüche berechnet hat.

Nimmt man die reducirte Form (1, 8, — 15), so findet man folgende Zahlen (§. 79)

$$k_0 = 1,\ k_1 = 7,\ k_2 = 1,\ k_3 = 16;$$

also die Näherungsbrüche

$$\frac{1}{1},\ \frac{8}{7},\ \frac{9}{8},\ \frac{152}{135};$$

die beiden letzten liefern die Substitution $\begin{pmatrix}8, & 135\\ 9, & 152\end{pmatrix}$, und hieraus ergiebt sich wieder $U = 9$, $T = 80$, wie vorher.

Beispiel 2: Es sei $D = 13 \equiv 1 \pmod{4}$; um die kleinste Auflösung der Gleichung $t^2 - 13u^2 = 4$ zu finden, nehmen wir die reducirte Form (2, 3, — 2), so ist (§. 79)

$$k_0 = 3, \; k_1 = 3;$$

die Näherungsbrüche sind also $\frac{3}{1}$ und $\frac{10}{3}$; dadurch erhalten wir die Substitution $\begin{pmatrix} 1, & 3 \\ 3, & 10 \end{pmatrix}$ und hieraus $U = 3$, $T = 11$.

§. 85.

Nachdem wir gezeigt haben, wie die kleinste positive Auflösung (T, U) der unbestimmten Gleichung immer gefunden werden kann, gehen wir dazu über, alle andern Auflösungen (t, u) auf diese eine zurückzuführen. Der Bequemlichkeit halber wollen wir, wenn t, u irgend zwei (positive oder negative) der Gleichung $t^2 - Du^2 = \sigma^2$ genügende Zahlen sind, und $\sqrt{D}$ stets positiv genommen wird, die Ausdrücke

$$\frac{t + u\sqrt{D}}{\sigma}, \quad \frac{t - u\sqrt{D}}{\sigma}$$

die zu dieser Auflösung (t, u) gehörigen Factoren nennen und als ersten und zweiten Factor von einander unterscheiden; das Product beider ist stets $= 1$; sie haben daher immer gleiche Zeichen, und zwar das positive oder negative, je nachdem t positiv oder negativ ist; haben ferner t und u gleiche Zeichen, so ist der erste Factor numerisch grösser als der zweite, folglich ist dann der erste numerisch > 1, der zweite numerisch < 1; das Gegentheil findet Statt, wenn t und u entgegengesetzte Zeichen haben; und wenn $u = 0$ ist, sind beide Factoren $= \pm 1$. Ist also z. B. (t, u) eine aus zwei positiven Zahlen bestehende Auflösung, so ist ihr erster Factor ein positiver unechter, und folglich ihr zweiter Factor ein positiver echter Bruch; und dies gilt auch umgekehrt: ist der erste Factor ein positiver unechter Bruch, so sind beide Zahlen t, u positiv.

Sind (t', u') und (t'', u'') irgend zwei identische oder verschiedene Auflösungen, so kann man

$$\frac{t' + u'\sqrt{D}}{\sigma} \cdot \frac{t'' + u''\sqrt{D}}{\sigma} = \frac{t + u\sqrt{D}}{\sigma}$$

setzen, wo (t, u) wieder eine Auflösung bedeutet. Denn entwickelt man das Product links und trennt das Rationale vom Irrationalen, so findet man

$$t = \frac{t't'' + Du'u''}{\sigma}, \quad u = \frac{t'u'' + u't''}{\sigma};$$

sollte $\sigma = 2$, also $D \equiv 1 \pmod{4}$ sein, so sind, wie man unmittelbar aus der unbestimmten Gleichung erkennt, die beiden, eine Auflösung bildenden, Zahlen t', u' entweder beide gerade, oder beide ungerade; und da dasselbe von t'', u'' gilt, so leuchtet ein, dass t und u auch in diesem Fall ganze Zahlen sind. Da nun aus der obigen Gleichung unmittelbar durch Verwandlung von $\sqrt{D}$ in $-\sqrt{D}$ oder auch durch den blossen Anblick der Ausdrücke für t, u die andere Gleichung

$$\frac{t' - u'\sqrt{D}}{\sigma} \cdot \frac{t'' - u''\sqrt{D}}{\sigma} = \frac{t - u\sqrt{D}}{\sigma}$$

folgt, so ergiebt sich durch Multiplication beider

$$\frac{t + u\sqrt{D}}{\sigma} \cdot \frac{t - u\sqrt{D}}{\sigma} = 1,$$

d. h. t und u bilden in der That eine Auflösung der unbestimmten Gleichung.

Dieser Satz lässt sich ohne Weiteres auf beliebig viele Auflösungen (t', u'), (t'', u''), (t''', u''') . . . ausdehnen: setzt man

$$\frac{t' + u'\sqrt{D}}{\sigma} \cdot \frac{t'' + u''\sqrt{D}}{\sigma} \cdot \frac{t''' + u'''\sqrt{D}}{\sigma} \cdots = \frac{t + u\sqrt{D}}{\sigma},$$

so wird (t, u) stets wieder eine ganzzahlige Auflösung sein. Bestehen ferner alle jene Auflösungen aus zwei positiven Zahlen, so sind alle Factoren linker Hand positive unechte Brüche; dasselbe gilt also auch von dem ersten Factor der Auflösung (t, u), und folglich sind t, u zwei positive Zahlen.

Setzen wir alle die einzelnen Auflösungen (t', u'), (t'', u'') . . . identisch mit der kleinsten positiven Auflösung (T, U), so können wir

$$\left(\frac{T + U\sqrt{D}}{\sigma}\right)^n = \frac{t_n + u_n\sqrt{D}}{\sigma}$$

setzen, wo n eine beliebige positive ganze Zahl bedeutet, und es

wird dann (t_n, u_n) jedesmal eine positive Auflösung werden; zugleich leuchtet ein, dass mit wachsendem Exponenten n der Werth der linker Hand stehenden Potenz eines unechten Bruchs, und folglich auch $t_n + u_n \sqrt{D}$ beständig wächst, so dass verschiedene Werthe von n auch verschiedene Auflösungen (t_n, u_n) liefern; und da die beiden Zahlen t_n, u_n entweder beide gleichzeitig wachsen, oder beide gleichzeitig abnehmen, so tritt offenbar das erstere oder letztere ein, je nachdem n wächst oder abnimmt.

Umgekehrt können wir zeigen, dass durch die vorstehende Formel in der That jede positive Auflösung (t, u) geliefert wird. Denn wäre der erste Factor einer solchen Auflösung keine genaue Potenz des ersten Factors der kleinsten Auflösung (T, U), so müsste er, da beide positive unechte Brüche sind, zwischen zwei successiven Potenzen

$$\left(\frac{T + U\sqrt{D}}{\sigma}\right)^n \text{ und } \left(\frac{T + U\sqrt{D}}{\sigma}\right)^{n+1}$$

des letztern liegen, wo n mindestens $= 1$ ist, da $\frac{t + u\sqrt{D}}{\sigma}$ nicht kleiner sein kann als $\frac{T + U\sqrt{D}}{\sigma}$. Dann wäre also

$$\frac{t_n + u_n\sqrt{D}}{\sigma} < \frac{t + u\sqrt{D}}{\sigma} < \frac{t_n + u_n\sqrt{D}}{\sigma} \cdot \frac{T + U\sqrt{D}}{\sigma};$$

multiplicirt man mit dem positiven Factor $\frac{t_n - u_n\sqrt{D}}{\sigma}$ und setzt

$$\frac{t + u\sqrt{D}}{\sigma} \cdot \frac{t_n - u_n\sqrt{D}}{\sigma} = \frac{t' + u'\sqrt{D}}{\sigma},$$

so würde

$$1 < \frac{t' + u'\sqrt{D}}{\sigma} < \frac{T + U\sqrt{D}}{\sigma}$$

folgen; es existirte daher eine positive Auflösung (t', u'), welche aus kleineren Zahlen t', u' bestände, als die kleinste Auflösung (T, U); was unmöglich ist.

Man findet daher alle aus zwei positiven Zahlen bestehenden Auflösungen durch die Formeln

$$\frac{t_n}{\sigma} = \frac{1}{\sigma^n} \left\{ T^n + \frac{n(n-1)}{1 \cdot 2} T^{n-2} U^2 D + \ldots \right\}$$

$$\frac{u_n}{\sigma} = \frac{1}{\sigma^n} \left\{ \frac{n}{1} T^{n-1} U + \frac{n(n-1)(n-2)}{1 \cdot 2 \cdot 3} T^{n-3} U^3 D + \ldots \right\}$$

wenn man der Reihe nach für n alle positiven ganzen Zahlen setzt. Da nun ferner

$$\frac{t_n - u_n \sqrt{D}}{\sigma} = \left(\frac{T - U\sqrt{D}}{\sigma}\right)^n = \left(\frac{T + U\sqrt{D}}{\sigma}\right)^{-n}$$

ist, so ergiebt sich, dass durch die Formel

$$\frac{t_n + u_n \sqrt{D}}{\sigma} = \left(\frac{T + U\sqrt{D}}{\sigma}\right)^n$$

sämmtliche Auflösungen t_n, u_n gegeben sind, in welchen t_n positiv ist, wenn man für n alle ganzen positiven und negativen Zahlen setzt, indem $u_{-n} = -u_n$, $t_{-n} = t_n$ ist. Für $n = 0$ ergiebt sich ferner $t_0 = +\sigma$, $u_0 = 0$. Will man daher alle Auflösungen t, u ohne Ausnahme in eine Formel zusammendrängen, so braucht man nur

$$\frac{t + u\sqrt{D}}{\sigma} = \pm \left(\frac{T + U\sqrt{D}}{\sigma}\right)^n$$

zu setzen, und hierin jedes der beiden Vorzeichen mit jedem ganzzahligen Exponenten n zu combiniren. Dass auf diese Weise keine Auflösung übergangen, und jede nur einmal erzeugt wird, folgt unmittelbar daraus, dass unter den vier verschiedenen Auflösungen

$$(t, u), (t, -u), (-t, u), (-t, -u)$$

wenn u nicht $= 0$ ist, immer eine und nur eine aus zwei positiven Zahlen besteht.

Hiermit ist nun das zweite Hauptproblem der Lehre von der Aequivalenz auch für ursprüngliche Formen von positiver Determinante vollständig gelöst. Wir sind durch die vollständige Auflösung der unbestimmten Gleichung $t^2 - Du^2 = \sigma^2$ in den Stand gesetzt, alle Transformationen einer solchen Form in sich selbst, und folglich auch alle Transformationen einer Form in eine äquivalente aus einer einzigen gegebenen solchen Transformation zu finden (§§. 60, 61).

Fünfter Abschnitt.

Bestimmung der Anzahl der Classen, in welche die binären quadratischen Formen von gegebener Determinante zerfallen.

§. 86.

Wir schreiten nun, nachdem die elementaren Theile der Theorie der quadratischen Formen behandelt sind, zu tieferen Untersuchungen, und namentlich zur Bestimmung der Classenanzahl der nicht äquivalenten Formen von einer gegebenen Determinante. Wir beschränken uns dabei auf ursprüngliche Formen der ersten oder zweiten Art, ferner, wenn die Determinante negativ ist, auf die Formen mit positiven äussern Coefficienten, da die Classenanzahl der andern Formen offenbar genau ebenso gross ist. Unter diesen Beschränkungen denken wir uns ein vollständiges Formensystem S der σten Art für die Determinante D gebildet. Zur Bestimmung der Anzahl der in diesem System S enthaltenen Formen führt die Betrachtung und genaue Definition aller durch sie darstellbaren Zahlen. Da durch eine Form der zweiten Art nur gerade Zahlen dargestellt werden können, so bezeichnen wir, um beide Fälle zusammenzufassen, die darstellbaren Zahlen allgemein mit σm, und ausserdem beschränken wir uns auf die Betrachtung derjenigen, in welchen m positiv, ungerade und relative Primzahl gegen die Determinante D ist. Endlich behalten wir das Wort „Darstellung" vorläufig noch in

dem frühern Sinn bei, nach welchem die beiden darstellenden Zahlen α, γ relative Primzahlen waren (§. 59).

Um den Charakter dieser Zahlen m genau festzustellen, erinnern wir uns, dass die Determinante D quadratischer Rest von jeder darstellbaren Zahl σm, d. h. dass die Congruenz

$$z^2 \equiv D \text{ (mod. } \sigma m)$$

möglich ist (§. 59). Es können daher in der ungeraden Zahl m nur solche Primzahlen f aufgehen, für welche

$$\left(\frac{D}{f}\right) = 1$$

ist. Umgekehrt: enthält m nur solche Primzahlen f, und ist die Anzahl der verschiedenen unter ihnen $= \mu$ (wo der Fall $\mu = 0$ nicht ausgeschlossen bleibt), so ist D quadratischer Rest von m, also auch von σm, und die obige Congruenz hat genau 2^μ incongruente Wurzeln (§. 37). Ist n ein bestimmter Repräsentant einer bestimmten dieser Wurzeln, so ist die Form $\left(\sigma m,\ n,\ \frac{n^2 - D}{\sigma m}\right)$ eine ursprüngliche Form der σten Art von der Determinante D *). Diese Form ist daher einer und nur einer in dem System S enthaltenen Form äquivalent **). Ist (a, b, c) diese Form des Systems, so liefert nur sie solche Darstellungen (α, γ) der Zahl σm, welche zu der durch n repräsentirten Wurzel der obigen Congruenz gehören, und zwar ebenso viele verschiedene solche Darstellungen (α, γ), als es Transformationen $\begin{pmatrix}\alpha, & \beta \\ \gamma, & \delta\end{pmatrix}$ der Form (a, b, c) in die Form $\left(\sigma m,\ n,\ \frac{n^2 - D}{\sigma m}\right)$, d. h. ebenso viele, als es Auflösungen (t, u) der unbestimmten Gleichung $t^2 - Du^2 = \sigma^2$ giebt (§§. 59, 60, 61). Den Complex aller dieser Darstellungen der Zahl σm, welche zu einer und derselben durch n repräsentirten Wurzel der obigen Congruenz gehören, wollen wir eine *Gruppe*

---

*) Man überzeugt sich hiervon leicht, wenn man bedenkt, dass m relative Primzahl zu $2D$, und dass ausserdem, wenn $\sigma = 2$, immer $D \equiv 1$ (mod. 4) ist.

**) Da der Coefficient σm positiv ist, so gilt dies auch für den Fall, in welchem D negativ ist, und also S nur Formen mit positiven äussern Coefficienten enthält.

von Darstellungen nennen. Den 2^μ incongruenten Wurzeln dieser Congruenz entsprechen daher 2^μ solche Gruppen von Darstellungen derselben Zahl σm durch Formen des Systems S, und in jeder Gruppe sind ebenso viele Darstellungen enthalten, als es Auflösungen der Gleichung $t^2 - Du^2 = \sigma^2$ giebt.

Das System der Zahlen m ist nun also vollständig definirt durch die Bedingungen:

1) *m ist positiv;*
2) *m ist relative Primzahl gegen $2D$;*
3) *D ist quadratischer Rest von m.*

§. 87.

Jetzt haben wir die Darstellungen von σm, welche einer und derselben Gruppe angehören, genauer zu betrachten.

Für den Fall einer *negativen* Determinante D ist die Anzahl $\varkappa$ der Auflösungen (t, u) der unbestimmten Gleichung $t^2 - Du^2 = \sigma^2$ endlich; dieselbe ist zugleich die Anzahl aller zu einer Gruppe gehörenden Darstellungen einer jeden Zahl σm; bedeutet also μ wieder die Anzahl der verschiedenen in m aufgehenden Primzahlen f, so ist 2^μ die Anzahl der Gruppen, deren jede $\varkappa$ Darstellungen enthält, und folglich ist

$$\varkappa \cdot 2^\mu$$

die Gesammtanzahl aller Darstellungen der Zahl σm; und hierin ist (§. 61)

$$\varkappa = 2 \text{ im Allgemeinen;}$$
$$\varkappa = 4, \text{ wenn } D = -1,$$
$$\varkappa = 6, \text{ wenn } D = -3 \text{ und } \sigma = 2$$

ist.

Für den Fall einer *positiven* Determinante D dagegen ist die Anzahl der Auflösungen (t, u) der unbestimmten Gleichung $t^2 - Du^2 = \sigma^2$, und folglich auch die Anzahl der in jeder der 2^μ Gruppen enthaltenen Darstellungen der Zahl σm unendlich gross. Wir gehen daher zunächst darauf aus, durch neue Bedingungen, welche den darstellenden Zahlen aufzuerlegen sind, aus den unendlich vielen in einer Gruppe enthaltenen Darstellungen stets

eine einzige zu isoliren. Dazu betrachten wir die allgemeine Form aller derselben Gruppe angehörenden Darstellungen (x, y) der Zahl σm. Ist wieder (a, b, c) die Form des Systems S, mit welcher die Form $\left(\sigma m, n, \frac{n^2 - D}{\sigma m}\right)$ äquivalent ist, und ist $\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}$ eine bestimmte Transformation der erstern Form in die letztere, so erhält man (nach §. 60) aus dieser einen alle andern durch die Zusammensetzung

$$\begin{pmatrix}\lambda, & \mu\\ \nu, & \varrho\end{pmatrix}\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix} = \begin{pmatrix}\lambda\alpha + \mu\gamma, & \lambda\beta + \mu\delta\\ \nu\alpha + \varrho\gamma, & \nu\beta + \varrho\delta\end{pmatrix}$$

aller Substitutionen $\begin{pmatrix}\lambda, & \mu\\ \nu, & \varrho\end{pmatrix}$, durch welche (a, b, c) in sich selbst übergeht, mit dieser bestimmten Substitution $\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}$. Da nun (nach §. 59) jedesmal der erste und dritte Coefficient einer solchen Substitution eine zu der Wurzel n gehörende Darstellung liefern, und da auch umgekehrt jede solche Darstellung (x, y) auf diese Weise, und zwar nur ein einziges Mal erzeugt wird, so ist die allgemeine Form aller dieser Darstellungen folgende:

$$x = \lambda\alpha + \mu\gamma, \quad y = \nu\alpha + \varrho\gamma;$$

da (α, γ) selbst eine solche Darstellung ist, so kann man sagen, dass diese beiden Gleichungen aus einer bestimmten Darstellung (α, γ) alle derselben Gruppe angehörenden Darstellungen (x, y) finden lehren. Nun war aber (§. 61)

$$\lambda = \frac{t - bu}{\sigma}, \quad \mu = -\frac{cu}{\sigma},$$

$$\nu = \frac{au}{\sigma}, \quad \varrho = \frac{t + bu}{\sigma},$$

wo (t, u) jede beliebige Auflösung der Gleichung $t^2 - Du^2 = \sigma^2$ bedeutete; folglich erhalten wir

$$x = \alpha\frac{t}{\sigma} - (b\alpha + c\gamma)\frac{u}{\sigma}, \quad y = \gamma\frac{t}{\sigma} + (a\alpha + b\gamma)\frac{u}{\sigma}\cdot$$

Für alle diese Werthe ist daher

$$ax^2 + 2bxy + cy^2 = \sigma m;$$

durch Multiplication mit dem ersten Coefficienten ergiebt sich

wie früher

$$\sigma a m = (a x + (b + \sqrt{D}) y) \ (a x + (b - \sqrt{D}) y),$$

und es tritt nun die höchst merkwürdige Erscheinung auf, dass jeder der beiden irrationalen Factoren rechter Hand eine geometrische Reihe constituirt; setzt man nämlich die vorstehenden Werthe von x, y ein, so ergiebt sich leicht

$$a x + (b + \sqrt{D}) y = (a \alpha + (b + \sqrt{D}) \gamma) \frac{t + u \sqrt{D}}{\sigma},$$

$$a x + (b - \sqrt{D}) y = (a \alpha + (b - \sqrt{D}) \gamma) \frac{t - u \sqrt{D}}{\sigma};$$

wenn man also mit T, U wie früher die kleinsten positiven Werthe von t, u bezeichnet und zur Abkürzung den positiven unechten Bruch

$$\frac{T + U \sqrt{D}}{\sigma} = \theta$$

setzt, so ist (nach §. 85)

$$a x + (b + \sqrt{D}) y = \pm (a \alpha + (b + \sqrt{D}) \gamma) \theta^{n}$$
$$a x + (b - \sqrt{D}) y = \pm (a \alpha + (b - \sqrt{D}) \gamma) \theta^{-n}$$

wo n eine beliebige positive oder negative ganze Zahl oder Null sein kann. Wir betrachten nur die erste dieser beiden Gleichungen, da aus ihr die zweite schon von selbst folgt. Ist nun k irgend ein von Null verschiedener reeller Zahlwerth, so leuchtet ein, dass man das Vorzeichen der rechten Seite und den Exponenten n stets und nur auf eine einzige Weise so bestimmen kann, dass der algebraische Werth von $a x + (b + \sqrt{D}) y$ zwischen den Grenzen k und $k\theta$ liegt; denn nachdem das Zeichen $\pm$ so gewählt ist, dass $\pm (a \alpha + (b + \sqrt{D}) \gamma)$ gleichstimmig mit k wird, giebt es nur noch ein einziges Glied der geometrischen Reihe zwischen den beiden vorgeschriebenen Grenzen, wenn man, um für jeden Fall Unbestimmtheit zu vermeiden, die eine derselben, z. B. $k\theta$, von dem Intervall ausschliesst. Durch diese Forderung für den Werth von $a x + (b + \sqrt{D}) y$ ist dann aus der unendlichen Anzahl von Darstellungen (x, y) eine einzige vollständig isolirt. Es kommt jetzt nur noch darauf an, k zweckmässig zu wählen.

Dazu können wir immer voraussetzen, dass die, eine ganze Classe repräsentirende, Form (a, b, c) des Systems S einen *positiven* ersten Coefficienten a hat; denn es giebt ja in jeder Classe sogar reducirte Formen, welche diese Eigenschaft haben. Wir machen daher von jetzt ab diese Voraussetzung über die Wahl der in S enthaltenen Formen (für negative Determinanten haben wir schon früher dieselbe Forderung gemacht, um dort die eine Hälfte aller Classen ganz von der Betrachtung auszuschliessen) und müssen sie dann natürlich für alles Folgende festhalten. Dann wählen wir für k die *positive* Quadratwurzel aus $\sigma a m$, was gestattet ist, da wir nur die positiven darstellbaren Zahlen σm betrachten. Wir stellen also die Bedingungen

$$\sqrt{\sigma a m} \leqq a x + (b + \sqrt{D})\, y < \theta \sqrt{\sigma a m}$$

auf, um aus allen derselben Gruppe angehörigen Darstellungen von σm durch (a, b, c) eine einzige (x, y) zu isoliren. Sie lassen sich, da ihre drei Glieder positiv sind, so umformen: quadrirt man, und bedenkt, dass $\sigma a m$ das Product aus zwei positiven irrationalen Factoren ist, so erhält man leicht durch Division

$$a x + (b - \sqrt{D})\, y \leqq a x + (b + \sqrt{D})\, y < \theta^2 (a x + (b - \sqrt{D})\, y);$$

durch Vergleichung der beiden ersten Glieder ergiebt sich die Bedingung

$$y \geqq 0;$$

die beiden letzten Glieder geben durch Umstellung und Restitution des Werthes von θ die Bedingung

$$a x + b y > \frac{T}{U}\, y.$$

Umgekehrt überzeugt man sich leicht, dass aus diesen beiden Bedingungen

$$y \geqq 0, \quad a x + b y > \frac{T}{U}\, y$$

rückwärts die obigen ursprünglichen Isolirungsbedingungen folgen.

Ausserdem zeigt sich, was besonders zu bemerken ist, dass in Folge dieser beiden Bedingungen auch der Werth der Form $a x^2 + 2 b x y + c y^2$ von selbst positiv ausfällt; denn da $T > U \sqrt{D}$

ist, so ergiebt sich durch Addition von $\pm y\sqrt{D}$ auf beiden Seiten der zweiten Bedingung, dass die beiden Factoren

$$ax + (b + \sqrt{D})\, y, \quad ax + (b - \sqrt{D})\, y$$

positiv sind, woraus dasselbe für ihr Product und also, da a positiv ist, auch für $ax^2 + 2bxy + cy^2$ folgt (für Formen von negativer Determinante versteht sich dies von selbst, da wir nur solche betrachten, deren äussere Coefficienten positiv sind).

§. 88.

Mit Rücksicht auf diese letzte Bemerkung können wir nun das Vorhergehende in folgender Weise noch einmal zusammenfassen:

Es sei S ein vollständiges System ursprünglicher Formen

$$(a, b, c), \quad (a', b', c') \ldots$$

der σten Art für eine gegebene Determinante D, mit positiven ersten Coefficienten $a, a' \ldots$ Dann setze man in jede dieser Formen, z. B. (a, b, c), für die Variabeln alle ganzzahligen Werthenpaare x, y ein, welche folgenden Bedingungen genügen:

I) $\dfrac{ax^2 + 2bxy + cy^2}{\sigma}$ *ist relative Primzahl zu* $2D$;

II) *im Fall einer positiven Determinante D ist*

$$y \geqq 0, \quad ax + by > \frac{T}{U}\, y$$

wo T, U die kleinsten positiven der Gleichung

$$T^2 - DU^2 = \sigma^2$$

genügenden ganzen Zahlen bedeuten;

III) *x und y sind relative Primzahlen zu einander.*

Auf diese Weise werden durch die Formen S alle ganzen Zahlen σm und nur solche dargestellt, welche folgenden Bedingungen genügen:

1) *m ist positiv*
2) *m ist relative Primzahl zu $2D$*
3) *D ist quadratischer Rest von m;*

und die Gesammtanzahl dieser Darstellungen einer jeden solchen Zahl σm ist gleich

$$\varkappa \cdot 2^{\mu},$$

wo μ die Anzahl der in m aufgehenden verschiedenen Primzahlen, und $\varkappa$ eine von m unabhängige Constante bedeutet, deren Werth $= 1$ für positive Determinanten, $= 4$ für $D = -1$, $= 6$ für $D = -3$ und $\sigma = 2$, und $= 2$ für die übrigen negativen Determinanten.

Dasselbe System der unendlich vielen Zahlen σm kann daher auf doppelte Art erzeugt werden, erstens durch Zusammensetzung aus den Primzahlen f, von welchen D quadratischer Rest ist, und zweitens durch die Substitution aller erlaubten Zahlenpaare x, y in die Formen des Systems S. Dieses Resultat der frühern Untersuchungen über die Aequivalenz der Formen und die Darstellbarkeit der Zahlen bildet das Grundprincip der folgenden Untersuchung. Wir bemerken zunächst, dass die Identität der auf die beiden verschiedenen Arten erzeugten Zahlensysteme nicht aufhören wird, wenn wir von jeder der erzeugten Zahlen eine bestimmte Function ψ nehmen, d. h. es wird wieder Identität bestehen zwischen dem Complex der Zahlen

$$\psi(ax^2 + 2bxy + cy^2), \quad \psi(a'x^2 + 2b'xy + c'y^2) \ldots$$

und dem System der Zahlen

$$\psi(\sigma m),$$

vorausgesetzt, dass der einem bestimmten Individuum σm entsprechende Functionswerth $\psi(\sigma m)$ genau $\varkappa \cdot 2^{\mu}$ mal in den letztern Complex aufgenommen wird. Ist daher die sonst ganz beliebige Function ψ so gewählt, dass die *Summe* aller dieser Werthe eine von der Anordnung derselben unabhängige convergente Reihe bildet, so folgt aus der angegebenen Identität die Fundamentalgleichung

$$\Sigma\, \psi(ax^2 + 2bxy + cy^2) + \Sigma\, \psi(a'x^2 + 2b'xy + c'y^2) + \cdots$$
$$= \varkappa\, \Sigma\, 2^{\mu}\, \psi(\sigma m).$$

Die linke Seite derselben besteht aus ebensoviel Hauptsummen, als das System S Formen (a, b, c), (a', b', c') enthält, d. h. als es Formenclassen für diese Determinante giebt. Jede Hauptsumme, wie z. B.

$$\Sigma\, \psi(ax^2 + 2bxy + cy^2)$$

ist eine doppelt unendliche Reihe, deren Glieder den sämmtlichen durch die Bedingungen I), II), III) definirten Zahlenpaaren x, y entsprechen (die Bedingungen I) und II) sind natürlich für die folgende Hauptsumme so zu modificiren, dass (a', b', c') an die Stelle von (a, b, c) tritt). Endlich bezieht sich die rechts angedeutete Summation auf alle aus den Primzahlen f zusammengesetzten Zahlen m, und ebenso behalten μ und $\varkappa$ ihre frühere Bedeutung. Wir specialisiren nun die Function ψ so, dass wir

$$\psi(z) = \frac{1}{z^s}$$

setzen, wo s ein beliebiger positiver Werth, aber > 1 ist; diese letztere Bedingung ist, wie wir später nachträglich zeigen werden, nothwendig, damit die vorstehenden unendlichen Reihen convergiren. Hierdurch geht unsere obige Gleichung in die folgende über:

$$\Sigma \left(\frac{ax^2 + 2bxy + cy^2}{\sigma}\right)^{-s} + \cdots = \varkappa\, \Sigma\, \frac{2^\mu}{m^s},$$

wo der Bequemlichkeit halber links nur eine einzige der den verschiedenen Formen entsprechenden Hauptsummen aufgeschrieben ist.

§. 89.

Wir beschäftigen uns nun zunächst mit einer Umformung der rechten Seite dieser Gleichung; zu dem Zweck betrachten wir das System

$$f_1,\ f_2,\ f_3 \cdots$$

der sämmtlichen Primzahlen f, welche nicht in $2D$ aufgehen, und von welchen D quadratischer Rest ist. Jede der oben definirten Zahlen m ist dann von der Form

$$f_1^{n_1}\, f_2^{n_2}\, f_3^{n_3} \ldots,$$

wo die Exponenten $n_1, n_2, n_3 \ldots$ positive ganze Zahlen oder Null

sind, und jedes m kann auch nur auf eine einzige Weise in diese Form gebracht werden. Bilden wir nun die diesen Primzahlen entsprechenden unendlichen Reihen

$$1 + \frac{2}{f_1^s} + \frac{2}{f_1^{2s}} + \frac{2}{f_1^{3s}} + \cdots + \frac{2}{f_1^{n_1 s}} + \cdots$$

$$1 + \frac{2}{f_2^s} + \frac{2}{f_2^{2s}} + \frac{2}{f_2^{3s}} + \cdots + \frac{2}{f_2^{n_2 s}} + \cdots$$

$$1 + \frac{2}{f_3^s} + \frac{2}{f_3^{2s}} + \frac{2}{f_3^{3s}} + \cdots + \frac{2}{f_3^{n_3 s}} + \cdots$$

u. s. w.

so erkennt man leicht mit Berücksichtigung der eben gemachten Bemerkung, dass das Product aller dieser Reihen nichts Anderes als die Summe

$$\Sigma \frac{2^\mu}{m^s}$$

ist. Denn das Product aus beliebigen Gliedern der ersten, zweiten, dritten Reihe u. s. f. hat die Form

$$\frac{2^\mu}{(f_1^{n_1} f_2^{n_2} f_3^{n_3} \ldots)^s} = \frac{2^\mu}{m^s}$$

wo μ die Anzahl der wirklich in m aufgehenden Primzahlen f bedeutet, d. h. derjenigen, deren Exponent n von Null verschieden ist; es entsteht daher auf diese Weise wirklich jedes Glied der genannten Reihe, und jedes auch nur ein einziges Mal. Da nun andererseits

$$1 + \frac{2}{f^s} + \frac{2}{f^{2s}} + \frac{2}{f^{3s}} + \cdots + \frac{2}{f^{ns}} + \cdots$$

$$= 1 + \frac{2}{f^s} \cdot \frac{1}{1 - \frac{1}{f^s}} = \frac{1 + \frac{1}{f^s}}{1 - \frac{1}{f^s}}$$

ist, so erhalten wir folgende Gleichung

$$\Sigma \frac{2^\mu}{m^s} = \Pi \frac{1 + \frac{1}{f^s}}{1 - \frac{1}{f^s}},$$

in welcher das Productzeichen Π sich auf die sämmtlichen oben definirten Primzahlen f bezieht.

Bezeichnen wir mit q allgemein *jede positive nicht in* $2D$ *aufgehende Primzahl*, so leuchtet ein, dass man die vorstehende Gleichung auch in folgender Form schreiben kann:

$$\Sigma \frac{2^\mu}{m^s} = \Pi \frac{1 + \frac{1}{q^s}}{1 - \left(\frac{D}{q}\right)\frac{1}{q^s}};$$

denn so oft q nicht zu den Primzahlen f gehört, reducirt sich der entsprechende Factor des Productes auf $+1$. In der so erhaltenen Gleichung multipliciren wir Zähler und Nenner des allgemeinen Factors zur Rechten mit $1 - \frac{1}{q^s}$, wodurch derselbe gleich

$$\frac{1 - \frac{1}{q^{2s}}}{\left(1 - \frac{1}{q^s}\right)\left(1 - \left(\frac{D}{q}\right)\frac{1}{q^s}\right)} = \frac{\left(\frac{1}{1 - \frac{1}{q^s}}\right) \cdot \left(\frac{1}{1 - \left(\frac{D}{q}\right)\frac{1}{q^s}}\right)}{\left(\frac{1}{1 - \frac{1}{q^{2s}}}\right)}$$

wird, und indem wir das unendliche Product in drei unendliche Producte zerlegen, erhalten wir

$$\Sigma \frac{2^\mu}{m^s} = \frac{\Pi \frac{1}{1 - \frac{1}{q^s}} \cdot \Pi \frac{1}{1 - \left(\frac{D}{q}\right)\frac{1}{q^s}}}{\Pi \frac{1}{1 - \frac{1}{q^{2s}}}}.$$

Jetzt können wir endlich jedes der drei rechts befindlichen Producte wieder in eine unendliche Reihe verwandeln. Da nämlich

$$\frac{1}{1 - \left(\frac{D}{q}\right)\frac{1}{q^s}} = \Sigma \left(\frac{D}{q}\right)^r \frac{1}{q^{rs}} =$$

$$1 + \left(\frac{D}{q}\right)\frac{1}{q^s} + \left(\frac{D}{q}\right)^2 \frac{1}{q^{2s}} + \cdots + \left(\frac{D}{q}\right)^r \frac{1}{q^{rs}} + \cdots$$

ist, so wird, wenn man für q alle, nicht in $2D$ aufgehenden, Primzahlen

$$q_1, q_2, q_3 \dots$$

setzt, das Product aller dieser Factoren gleich der Summe aller Glieder von der Form

$$\left(\frac{D}{q_1}\right)^{r_1} \left(\frac{D}{q_2}\right)^{r_2} \left(\frac{D}{q_3}\right)^{r_3} \dots \frac{1}{(q_1^{r_1} q_2^{r_2} q_3^{r_3} \dots)^s}$$

worin die Exponenten $r_1, r_2, r_3 \dots$ alle positiven ganzen Zahlen und Null zu durchlaufen haben. Das System aller der in den Nennern unter dem Exponenten s vorkommenden Zahlen

$$q_1^{r_1} q_2^{r_2} q_3^{r_3} \dots = n$$

besteht offenbar aus sämmtlichen *positiven ganzen Zahlen* n, *welche relative Primzahlen gegen* $2D$ *sind;* jede solche Zahl n wird einmal und auch nur einmal durch ein bestimmtes System von Exponenten $r_1, r_2, r_3 \dots$ erzeugt; gleichzeitig ist dann mit Benutzung der von *Jacobi* erweiterten Bedeutung des Legendre'schen Zeichens

$$\left(\frac{D}{q_1}\right)^{r_1} \left(\frac{D}{q_2}\right)^{r_2} \left(\frac{D}{q_3}\right)^{r_3} \dots = \left(\frac{D}{q_1^{r_1}}\right) \left(\frac{D}{q_2^{r_2}}\right) \left(\frac{D}{q_3^{r_3}}\right) \dots$$
$$= \left(\frac{D}{q_1^{r_1} q_2^{r_2} q_3^{r_3} \dots}\right) = \left(\frac{D}{n}\right).$$

Hierdurch gewinnen wir also folgende Verwandlung

$$\Pi \frac{1}{1 - \left(\frac{D}{q}\right) \frac{1}{q^s}} = \Sigma \left(\frac{D}{n}\right) \frac{1}{n^s},$$

wo das Summenzeichen rechts sich auf alle positiven Zahlen n bezieht, die relative Primzahlen gegen $2D$ sind.

Verfährt man ganz ebenso, indem man alle die Entwickelungen

$$\frac{1}{1 - \frac{1}{q^s}} = 1 + \frac{1}{q^s} + \frac{1}{q^{2s}} + \dots + \frac{1}{q^{rs}} + \dots$$

mit einander multiplicirt, so erhält man offenbar

$$\Pi \frac{1}{1-\frac{1}{q^s}} = \Sigma \frac{1}{n^s}$$

und folglich auch

$$\Pi \frac{1}{1-\frac{1}{q^{2s}}} = \Sigma \frac{1}{n^{2s}} .$$

Hierdurch haben wir die wichtige Umformung

$$\Sigma \frac{2^\mu}{m^s} = \frac{\Sigma \frac{1}{n^s} \times \Sigma \left(\frac{D}{n}\right) \frac{1}{n^s}}{\Sigma \frac{1}{n^{2s}}}$$

gewonnen*).

§. 90.

Wir multipliciren nun beide Seiten unserer Hauptgleichung mit der unendlichen Reihe

$$\Sigma \frac{1}{n^{2s}},$$

wodurch sie dem eben gewonnenen Resultat gemäss in die folgende übergeht:

$$\Sigma \frac{1}{n^{2s}} \times \Sigma \left(\frac{ax^2+2bxy+cy^2}{\sigma}\right)^{-s} + \cdots = \varkappa \Sigma \frac{1}{n^s} \times \Sigma \left(\frac{D}{n}\right) \frac{1}{n^s}.$$

Führen wir in dem ersten Gliede links die Multiplication der beiden Summen aus, so kann das Resultat als die dreifach unendliche Reihe

$$\Sigma \left(\frac{an^2x^2 + 2bn^2xy + cn^2y^2}{\sigma}\right)^{-s}$$

geschrieben werden, in welcher für x, y alle den frühern Bedingungen I), II), III) genügenden Werthe (§. 88), und für n alle positiven relativen Primzahlen gegen $2D$ zu setzen sind. Diese

*) Eine directe Verification dieser Gleichung ohne Benutzung unendlicher Producte findet man in §. 124.

Reihe kann man aber auch wieder als eine doppelt unendliche ansehen, wenn man

$$nx = x', \; ny = y'$$

setzt; denn dann nimmt sie die Gestalt

$$\Sigma \left(\frac{ax'^2 + 2bx'y' + cy'^2}{\sigma}\right)^{-s}$$

an, und es fragt sich nur, welche Bedingungen den neuen Summationsbuchstaben x', y' aufzuerlegen sind. Diese ergeben sich aus den Bedingungen für x, y, n folgendermassen. Erstens: Da x, y zufolge der Bedingung I) so gewählt werden müssen, dass

$$\frac{ax^2 + 2bxy + cy^2}{\sigma}$$

relative Primzahl gegen $2D$ wird, und da n ebenfalls relative Primzahl gegen $2D$ ist, so gilt dasselbe von

$$\frac{ax'^2 + 2bx'y' + cy'^2}{\sigma} = n^2 \cdot \frac{ax^2 + 2bxy + cy^2}{\sigma}.$$

Zweitens: für den Fall einer positiven Determinante waren x, y den Isolirungsbedingungen II)

$$y \geqq 0, \quad ax + by > \frac{T}{U}\, y$$

zu unterwerfen; multiplicirt man dieselben mit n, so ergeben sich die ganz gleichlautenden Bedingungen

$$y' \geqq 0, \quad ax' + by' > \frac{T}{U}\, y'.$$

Drittens: aus der Bedingung, dass x, y relative Primzahlen sein sollen, würde jetzt nur noch folgen, dass der grösste gemeinschaftliche Divisor n von x', y' relative Primzahl gegen $2D$ sien muss; allein diese Bedingung kann man gänzlich fallen lassen, da sie schon in der ersten enthalten ist; denn sobald x', y' einen gemeinschaftlichen Divisor hätten, der nicht relative Primzahl gegen $2D$ wäre, so könnte auch

$$\frac{ax'^2 + 2bx'y' + cy'^2}{\sigma}$$

nicht relative Primzahl gegen $2D$ sein.

Es zeigt sich also, dass die neuen Variabeln x', y' nur den beiden Bedingungen I) und II) zu unterwerfen sind, wenn man in denselben die Variabeln accentuirt, dass dagegen die Bedingung III) ganz fortgefallen ist. Umgekehrt überzeugt man sich leicht, dass ein jedes solches Werthenpaar x', y' einmal und nur einmal durch ein Werthenpaar x, y und eine Zahl n erzeugt wird.

Wir lassen nun der Bequemlichkeit halber die Accente der Variabeln wieder fort, und schreiben daher unsere Hauptgleichung in folgender Form

$$\Sigma \left(\frac{ax^2 + 2bxy + cy^2}{\sigma}\right)^{-s} + \cdots = \varkappa \Sigma \frac{1}{n^s} \times \Sigma \left(\frac{D}{n}\right) \frac{1}{n^s}$$

wo nun in der ersten auf die Form (a, b, c) bezüglichen Hauptsumme die Summationsbuchstaben nur noch den beiden folgenden Bedingungen zu unterwerfen sind:

I) Der Werth $\frac{ax^2 + 2bxy + cy^2}{\sigma}$ soll relative Primzahl gegen $2D$ sein.

II) Im Fall einer positiven Determinante soll

$$y \geqq 0, \quad ax + by > \frac{T}{U} y$$

sein, wo T, U die frühere Bedeutung haben.

§. 91.

Bevor wir weitergehen, wollen wir aus unserer letzten Gleichung einige interessante Folgerungen ziehen: die erste derselben ist rein zahlentheoretischer Natur und vervollständigt unsere frühere Theorie der Darstellung. Wir multipliciren die beiden unendlichen Reihen

$$\Sigma \frac{1}{n'^s}, \quad \Sigma \left(\frac{D}{n''}\right) \frac{1}{n''^s}$$

rechter Hand, nachdem wir die Summationsbuchstaben, um sie von einander zu unterscheiden, accentuirt haben; dann erhalten wir als Product die doppelt unendliche Reihe

$$\Sigma \left(\frac{D}{n''}\right) \frac{1}{(n'n'')^s},$$

in welcher sowohl n' als auch n'' das Gebiet aller Zahlen n, d. h. aller derjenigen positiven ganzen Zahlen zu durchlaufen hat, welche relative Primzahlen gegen $2D$ sind. Offenbar ist jedes Product von der Form $n'n''$ wieder in demselben Gebiet enthalten; fassen wir daher alle Glieder der Doppelsumme, in welchen das Product $n'n''$ denselben Werth n hat, immer in ein einziges zusammen, so können wir diese Doppelsumme wieder in die Form einer einfach unendlichen Reihe

$$\Sigma \frac{\tau}{n^s}$$

bringen; bezeichnet man mit δ die sämmtlichen Divisoren der Zahl n, so wird offenbar

$$\tau = \Sigma \left(\frac{D}{\delta}\right).$$

Dividiren wir ferner die Gleichung auf beiden Seiten durch σ^s, so nimmt sie folgende Form an

$$\Sigma \frac{1}{(ax^2 + 2bxy + cy^2)^s} + \cdots = \Sigma \frac{\varkappa\tau}{(\sigma n)^s}.$$

Fassen wir nun auch links alle in den verschiedenen Doppelsummen vorkommenden Glieder, welche denselben Werth haben, in ein einziges zusammen, so erhalten wir folgende Gleichung

$$\Sigma \frac{\lambda}{\nu^s} = \Sigma \frac{\varkappa\tau}{(\sigma n)^s},$$

wo mit ν alle die durch die sämmtlichen Formen $(a, b, c) \ldots$ des Systems S darstellbaren Zahlen bezeichnet werden, und λ die Anzahl der verschiedenen Darstellungen einer solchen Zahl ν bedeutet. Hierbei ist wohl zu bemerken, dass das Wort „Darstellung“ jetzt in einem allgemeinern Sinne gebraucht wird, als früher (§. 59), indem jetzt die darstellenden Zahlen x, y nur noch den Bedingungen I) und II) des vorigen Paragraphen unterworfen sind, während sie früher auch relative Primzahlen unter einander sein mussten.

Besteht nun für jeden über einer gewissen Grenze liegenden positiven Werth des Exponenten s eine Gleichung von der Form

$$\frac{\alpha}{a^s} + \frac{\beta}{b^s} + \frac{\gamma}{c^s} + \cdots = \frac{\alpha'}{a'^s} + \frac{\beta'}{b'^s} + \frac{\gamma'}{c'^s} + \cdots$$

wo $a, b, c \ldots$ sowohl wie $a', b', c' \ldots$ positive und in ihrer Aufeinanderfolge wachsende Zahlwerthe bedeuten, und sind die sämmtlichen Coefficienten $\alpha, \beta, \gamma \ldots \alpha', \beta', \gamma' \ldots$ von Null verschieden, so folgt hieraus die vollständige Identität beider Reihen, d. h. es ist

$$a = a', \quad b = b', \quad c = c' \ldots$$
$$\alpha = \alpha', \quad \beta = \beta', \quad \gamma = \gamma' \ldots$$

Um dies zu beweisen, können wir annehmen, es sei $a \leqq a'$; multipliciren wir beide Seiten der Gleichung mit a^s, so erhalten wir

$$\alpha + \beta\left(\frac{a}{b}\right)^s + \gamma\left(\frac{a}{c}\right)^s + \cdots$$
$$= \alpha'\left(\frac{a}{a'}\right)^s + \beta'\left(\frac{a}{b'}\right)^s + \gamma'\left(\frac{a}{c'}\right)^s + \cdots$$

Da nun sowohl die Werthe

$$\frac{a}{b}, \ \frac{a}{c} \ldots$$

als auch die Werthe

$$\frac{a}{b'}, \ \frac{a}{c'} \ldots$$

fortwährend abnehmende echte Brüche sind, und beide Reihen convergiren, so überzeugt man sich leicht *), dass mit unbegrenzt wachsendem s die linke Seite der vorstehenden Gleichung sich dem Grenzwerth α nähert, und ebenso die rechte dem Grenzwerth α' oder 0, je nachdem $a = a'$ oder $< a'$ ist. Da nun beide Seiten sich nothwendig demselben Grenzwerth nähern müssen, und α von Null verschieden ist, so muss $a = a'$, und folglich auch $\alpha = \alpha'$ sein. Nachdem so die Identität der ersten Glieder auf beiden Seiten bewiesen ist, kann man dieselben fortlassen; aus der so entstehenden Gleichung

$$\frac{\beta}{b^s} + \frac{\gamma}{c^s} + \cdots = \frac{\beta'}{b'^s} + \frac{\gamma'}{c'^s} + \cdots$$

folgt dann auf dieselbe Weise, dass $b = b'$ und $\beta = \beta'$ sein muss, und so kann man fortfahren.

*) Vergl. Supplement IX.

Wendet man dies Princip auf unsere obige Gleichung an, so ergiebt sich, dass jedes σn, dem ein von Null verschiedenes τ entspricht, nothwendig eine Zahl ν, d. h. eine durch die Formen S darstellbare Zahl, und dass die Anzahl λ der verschiedenen Darstellungen eines solchen $\nu = \sigma n$ gleich $\varkappa\tau$ ist; wenn dagegen $\tau = 0$ ist, so kann auch σn keine durch die Formen S darstellbare Zahl ν sein; wir können daher in beiden Fällen sagen, dass die Anzahl aller Darstellungen einer Zahl σn durch die Formen S immer

$$= \varkappa\tau = \varkappa \sum \left(\frac{D}{\delta}\right)$$

ist, wo δ alle Divisoren der Zahlen n durchlaufen muss.

Wir wollen dieses Resultat auf einige Beispiele anwenden.

1) Ist $D = -1$ (und folglich $\sigma = 1$), so ist nur eine einzige Form in dem System S enthalten, für welche wir die Form $(1, 0, 1)$ wählen können; das System der Zahlen σn ist das der positiven ungeraden Zahlen, und da $\varkappa = 4$ ist, so erhalten wir das Resultat:

Die Anzahl aller Darstellungen einer beliebigen positiven ungeraden Zahl n durch die Form $(1, 0, 1) = x^2 + y^2$ ist gleich

$$4 \sum (-1)^{\frac{1}{2}(\delta - 1)} = 4\,(M - N)$$

d. h. gleich dem vierfachen Ueberschuss der Anzahl M ihrer Divisoren δ von der Form $4h + 1$ über die Anzahl N der Divisoren δ von der Form $4h + 3$.

Die darstellenden Zahlen x, y sind gar keiner Beschränkung unterworfen; es leuchtet ferner ein, dass jedesmal acht verschiedene Darstellungen eine einzige Zerlegung in zwei Quadrate geben; nur wenn eine der beiden darstellenden Zahlen $= 0$ ist, findet eine Ausnahme Statt, weil dann nur vier verschiedene Darstellungen dieselbe Zerlegung liefern, ein Fall, der nur dann eintreten kann, wenn n eine Quadratzahl ist. Die Anzahl der verschiedenen Zerlegungen ist daher $\frac{1}{2}(M - N + 1)$ oder $\frac{1}{2}(M - N)$, e nachdem n eine Quadratzahl ist oder nicht. So ist z. B.

$$25 = 0^2 + 5^2 = 3^2 + 4^2$$
$$45 = 3^2 + 6^2$$
$$49 = 0^2 + 7^2$$
$$65 = 1^2 + 8^2 = 4^2 + 7^2.$$

Ist endlich n eine Primzahl, so ergiebt sich wieder, dass n

auf eine einzige, oder auf gar keine Weise in zwei Quadrate zerlegt werden kann, je nachdem n von der Form $4h+1$, oder von der Form $4h+3$ ist (§. 68).

2) Für die positive Determinante $D=2$ existiren nur die beiden einander äquivalenten reducirten Formen $(1, 1, -1)$ und $(-1, 1, 1)$, also nur eine einzige Classe; als repräsentirende Form kann man daher auch $(1, 0, -2) = x^2 - 2y^2$ wählen. Da die kleinsten der Gleichung $t^2 - 2u^2 = 1$ genügenden Zahlen $T=3$, $U=2$ sind, so werden nur solche Darstellungen betrachtet, in welchen $y \geqq 0$, $2x > 3y$ ist. Da ferner

$$\left(\frac{2}{\delta}\right) = (-1)^{\frac{1}{8}(\delta^2-1)} = +1 \text{ oder } = -1$$

ist, je nachdem $\delta = 8h \pm 1$ oder $\delta = 8h \pm 5$ ist, so bekommen wir folgendes Resultat:

Die Anzahl aller den obigen Bedingungen genügenden Darstellungen (x, y) einer beliebigen positiven ungeraden Zahl n durch die Form $x^2 - 2y^2$ ist gleich dem Ueberschuss der Anzahl der Divisoren von n, welche die Form $8h \pm 1$ haben, über die Anzahl der andern Divisoren.

§. 92.

Eine zweite interessante Anwendung der vorstehenden Untersuchung machen wir auf die Analysis. Wir haben gesehen, dass durch Einsetzen aller den Bedingungen I) und II) genügenden ganzzahligen Werthenpaare x, y in die Formen $(a, b, c)\dots$ des Systems S die Zahlen σn erzeugt werden, und zwar ist

$$\varkappa\tau = \varkappa\Sigma\left(\frac{D}{\delta}\right)$$

die Anzahl der verschiedenen Erzeugungen einer solchen Zahl σn, wenn wieder für δ alle Divisoren von n gesetzt werden. Nehmen wir daher von jeder der Zahlen $ax^2 + 2bxy + cy^2$ eine bestimmte Function ψ, so entsteht auf diese Weise jeder Werth $\psi(\sigma n)$ so oft als $\varkappa\tau$ angiebt. Hieraus folgt wieder, dass

$$\Sigma\,\psi(ax^2 + 2bxy + cy^2) + \cdots = \varkappa\,\Sigma\tau\,\psi(\sigma n)$$

sein wird, sobald die Function ψ so gewählt wird, dass diese unendlichen Reihen bestimmte von der Anordnung ihrer Glieder unabhängige Summen haben. Dies ist der Fall, wenn man

$$\psi(z) = q^z$$

setzt, wo q eine reelle oder complexe Grösse bedeutet, deren Modulus ein echter Bruch ist. Man erhält auf diese Weise folgende sehr allgemeine Gleichung

$$\sum q^{ax^2+2bxy+cy^2} + \cdots = \varkappa \sum \tau q^{\sigma n};$$

da auf der rechten Seite der Coefficient τ selbst wieder eine Summe ist, in welcher δ die sämmtlichen Divisoren von n zu durchlaufen hat, so kann man, indem man n in $n'\delta$ verwandelt, die Gleichung auch so schreiben

$$\sum q^{ax^2+2bxy+cy^2} + \cdots = \varkappa \sum \left(\frac{D}{\delta}\right) q^{\sigma n'\delta},$$

wo nun rechts eine Doppelsumme steht, in welcher jeder der beiden Summationsbuchstaben n' und δ das Gebiet aller Zahlen n zu durchlaufen hat.

Wir wollen die vorstehende Gleichung auf einige specielle Fälle anwenden. Nehmen wir z. B. $D = -1$, also $\sigma = 1$, so haben wir links nur eine einzige Doppelsumme; nehmen wir wieder $(1, 0, 1)$ als die repräsentirende Form, so ist dieselbe gleich

$$\sum q^{x^2+y^2},$$

worin x, y alle Werthenpaare zu durchlaufen haben, für welche $x^2 + y^2$ ungerade ausfällt; es muss daher eine der beiden Zahlen x, y ungerade, die andere gerade sein; da man nun in jeder erlaubten Combination x mit y vertauschen kann, so setzen wir fest, dass x nur die ungeraden, y nur die geraden Werthe durchlaufen soll, müssen dann aber die so beschränkte Doppelreihe mit 2 multipliciren; wir erhalten so

$$2 \sum q^{x^2+y^2} = 2 \sum q^{x^2} q^{y^2} = 2 \sum q^{x^2} \times \sum q^{y^2}$$

wo x alle positiven und negativen ungeraden, y alle positiven und negativen geraden Zahlen und Null zu durchlaufen hat; beschränken wir aber x auf alle positiven ungeraden, und y auf alle positiven geraden Zahlen, so können wir das vorstehende Product auch so schreiben

$$4 \Sigma q^{x^2} \times (1 + 2 \Sigma q^{y^2}).$$

Auf der rechten Seite haben wir die Doppelsumme

$$4 \Sigma \left(\frac{-1}{\delta}\right) q^{n'\delta} = 4 \Sigma (-1)^{\frac{1}{2}(\delta-1)} q^{n'\delta},$$

wo n' und δ alle positiven ungeraden Zahlen zu durchlaufen haben; die Summation in Bezug auf n' lässt sich ausführen, indem

$$\Sigma q^{n'\delta} = q^{\delta} + q^{3\delta} + q^{5\delta} + \cdots = \frac{q^{\delta}}{1 - q^{2\delta}}$$

ist; dadurch wird die rechte Seite gleich

$$4 \Sigma (-1)^{1/2(\delta-1)} \frac{q^{\delta}}{1 - q^{2\delta}}$$

und wir erhalten daher folgende merkwürdige Gleichung

$$(q + q^9 + q^{25} + q^{49} + \cdots)(1 + 2q^4 + 2q^{16} + 2q^{36} + \cdots)$$
$$= \frac{q}{1 - q^2} - \frac{q^3}{1 - q^6} + \frac{q^5}{1 - q^{10}} - \frac{q^7}{1 - q^{14}} + \cdots$$

welche, wie die andern Gleichungen, welche negativen Determinanten entsprechen, auch aus der Theorie der *Elliptischen Functionen* abgeleitet werden kann.

Für positive Determinanten fallen die entsprechenden Gleichungen weniger einfach aus, weil auf der linken Seite die Variabeln x, y immer noch der Bedingung II) unterworfen sind. Nehmen wir z. B. $D = 2$, also $\sigma = 1$, $\varkappa = 1$, so erhalten wir in ähnlicher Weise die Gleichung

$$\Sigma q^{x^2 - 2y^2} = \Sigma \left(\frac{2}{\delta}\right) q^{\delta n'}$$

$$= \frac{q}{1 - q^2} - \frac{q^3}{1 - q^6} - \frac{q^5}{1 - q^{10}} + \frac{q^7}{1 - q^{14}} + \cdots,$$

wo auf der linken Seite für x, y alle Werthenpaare zu setzen sind, die den Bedingungen $y \geqq 0$, $2x > 3y$ genügen und für welche ausserdem $x^2 - 2y^2$ und also x ungerade ist.

§. 93.

Wir kehren nun zu unserem eigentlichen Gegenstande, der weitern Behandlung der Gleichung (§. 90)

$$\Sigma\left(\frac{ax^2+2bxy+cy^2}{\sigma}\right)^{-s}+\cdots=\varkappa\,\Sigma\frac{1}{n^s}\times\Sigma\left(\frac{D}{n}\right)\frac{1}{n^s}$$

zurück, und es wird gut sein, den Gang der Untersuchung hier mit wenigen Worten im Voraus anzugeben. Man würde auf unübersteigliche Schwierigkeiten stossen, wenn man die auf der linken Seite angedeuteten Summationen für einen beliebigen Werth von $s > 1$ wirklich ausführen wollte. Lässt man dagegen den Exponenten s immer mehr abnehmen und gegen den Werth 1 convergiren, so wird gleichzeitig jede dieser Hauptsummen über alle Grenzen wachsen, und bei näherer Betrachtung zeigt sich, dass das Product aus einer solchen Hauptsumme und aus $(s-1)$ sich einem festen endlichen Grenzwerth L nähert, welcher nur von der allen Formen gemeinschaftlichen Determinante D abhängt, und folglich wird der Grenzwerth der ganzen mit $(s-1)$ multiplicirten linken Seite $= hL$ sein, wenn man mit h die Anzahl der Hauptsummen, d. h. also die Anzahl der in dem Formensystem S enthaltenen Formen (a, b, c) . . . bezeichnet. Da ferner der Grenzwerth der mit $(s-1)$ multiplicirten rechten Seite sich direct bestimmen lässt, so erhält man auf diese Weise einen Ausdruck für die Classenanzahl h, deren Bestimmung ja den Gegenstand unserer ganzen Untersuchung bildet.

Bevor wir aber dazu übergehen, diesen Grenzprocess durchzuführen, müssen wir noch einige vorläufige Fragen erörtern, deren Beantwortung für unsern Zweck durchaus erforderlich ist. Zunächst wenden wir uns dazu, die den Summationsbuchstaben x, y auferlegte Bedingung I) (§. 90) so umzuformen, dass man einen deutlichen Ueberblick über das System der ihr genügenden Werthenpaare x, y erhält. Zu dem Ende dürfen wir annehmen, dass der Repräsentant (a, b, c) einer ganzen Classe immer so gewählt ist, dass der Quotient $a : \sigma$ nicht nur, wie schon früher festgesetzt wurde, positiv, sondern auch *relative Primzahl gegen* $2D$ ist. Von der Berechtigung zu dieser Annahme wird man sich durch die folgende Betrachtung überzeugen. Ist

$$(a, b, c) = \sigma (Ax^2 + Bxy + Cy^2) = \sigma F$$

eine beliebige ursprüngliche Form von der σten Art, und r irgend eine Primzahl, so kann man den beiden Variabeln x, y der Form stets solche Werthe beilegen, dass der Werth von F nicht durch r theilbar wird; denn ist eine der beiden Zahlen A, C, z. B. A, nicht durch r theilbar, so gebe man x einen durch r nicht theilbaren, y dagegen einen durch r theilbaren Werth; sind aber beide Coefficienten A, C durch r theilbar, so ist B gewiss nicht durch r theilbar, und folglich genügt es dann, x und y Werthe beizulegen, die beide nicht durch r theilbar sind. Man kann folglich auch x und y immer so wählen, dass der Werth von F relative Primzahl gegen irgend eine vorgeschriebene Zahl k wird; denn bezeichnet man mit r', r'', r''' ... die sämmtlichen in k aufgehenden Primzahlen, so braucht man nur zu bewirken, dass F durch keine einzige derselben theilbar wird, was nach dem eben Gesagten sich stets dadurch erreichen lässt, dass die beiden Variabeln x, y durch einige dieser Primzahlen theilbar, durch andere nicht theilbar angenommen werden — Bedingungen, die sich stets auf unendlich viele verschiedene Arten erfüllen lassen. Man kann hinzufügen, dass x, y ausserdem noch so gewählt werden können, dass der Werth von F positiv ausfällt; für eine negative Determinante D versteht sich dies von selbst, da wir Formen mit negativen äussern Coefficienten ausschliessen; für eine positive Determinante braucht man, da

$$a\sigma F = (ax + by)^2 - Dy^2$$

ist, nur dafür zu sorgen, dass, je nachdem a positiv oder negativ ist, entsprechend $(ax + by)$ absolut genommen grösser oder kleiner als $y\sqrt{D}$ ausfällt, und offenbar lassen die bisher den Variabeln x, y auferlegten Bedingungen, durch einige Primzahlen theilbar, durch einige andere nicht theilbar zu sein, noch solchen Spielraum für ihr Grössenverhältniss, dass auch dieser Forderung noch auf unendlich viele verschiedene Arten genügt werden kann. Endlich können wir noch behaupten, dass für die Variabeln x, y auch solche Werthe gewählt werden können, welche unter einander relative Primzahlen sind und doch die übrigen Bedingungen erfüllen, dass F positiv und relative Primzahl gegen die vorgeschriebene Zahl k ist; denn haben x und y einen gemeinschaftlichen Divisor, so braucht man sie nur durch Division von demselben zu befreien, und die Quotienten, die unter einander rela-

tive Primzahlen sind, bilden ein solches allen Anforderungen genügendes Werthenpaar.

Wir machen von der vorstehenden (auch für andere Untersuchungen nützlichen) Betrachtung eine specielle Anwendung auf den Fall, in welchem $k = 2D$ ist; wir können dann so sagen: ist (a, b, c) irgend eine ursprüngliche Form der σten Art von der Determinante D, so kann man stets zwei relative Primzahlen α, γ von der Beschaffenheit finden, dass

$$\frac{a'}{\sigma} = \frac{a\alpha^2 + 2b\alpha\gamma + c\gamma^2}{\sigma}$$

positiv und relative Primzahl gegen $2D$ wird. Da nun α, γ relative Primzahlen sind, so kann man (§. 59) irgend ein Paar von Werthen β, δ wählen, welche der Gleichung $\alpha\delta - \beta\gamma = 1$ genügen, und dann geht die Form (a, b, c) durch die Substitution $\begin{pmatrix}\alpha, & \beta \\ \gamma, & \delta\end{pmatrix}$ in eine äquivalente Form über, deren erster Coefficient a' positiv ist und ausserdem die Eigenschaft hat, dass $a' : \sigma$ relative Primzahl gegen $2D$ ist. Und hiermit ist in der That der verlangte Nachweis geliefert, dass in jeder Formenclasse solche Repräsentanten ausgewählt werden können, welche die obige neue Bedingung erfüllen.

§. 94.

Wir nehmen daher jetzt an, dass die repräsentirende Form (a, b, c) so gewählt ist, dass $a : \sigma$ nicht nur positiv, sondern auch relative Primzahl gegen $2D$ ist, und fragen nun nach dem System aller Werthenpaare x, y, welche der Bedingung I) genügen, dass

$$\frac{ax^2 + 2bxy + cy^2}{\sigma}$$

relative Primzahl gegen $2D$ wird. Bezeichnen wir wie früher mit Δ den absoluten Werth der Determinante D, so kann man stets

$$x = 2\Delta v + \alpha, \quad y = 2\Delta w + \gamma$$

setzen, wo α und γ irgend welche der 2Δ Zahlen

$$0, 1, 2 \ldots (2\Delta - 1)$$

und v und w beliebige ganze reelle Zahlen bedeuten; jede Combination zweier ganzen Zahlen x, y kann stets und nur auf eine einzige Weise in diese Form gebracht werden. Da nun aus

$$x \equiv \alpha \pmod{2\Delta} \text{ und } y \equiv \gamma \pmod{2\Delta}$$

auch

$$\frac{ax^2 + 2bxy + cy^2}{\sigma} \equiv \frac{a\alpha^2 + 2b\alpha\gamma + c\gamma^2}{\sigma} \pmod{2\Delta}$$

folgt, so leuchtet ein, dass man unter den sämmtlichen $4\Delta^2$ Combinationen (α, γ) nur diejenigen zu ermitteln hat, für welche

$$\frac{a\alpha^2 + 2b\alpha\gamma + c\gamma^2}{\sigma}$$

relative Primzahl gegen 2Δ wird. Die gesuchten Combinationen (x, y) vertheilen sich dann in zusammengehörige Paare von arithmetischen Reihen, deren Differenz $= 2\Delta$ ist, und deren Anfangsglieder α, γ specielle solche Combinationen sind, die dieselbe Bedingung erfüllen. Uns kommt es nun weniger darauf an, wirklich alle diese Combinationen (α, γ) genau zu definiren, als vielmehr, nur ihre *Anzahl* sicher festzustellen, weil diese allein bei dem spätern Grenzübergang eine Rolle spielt. Hierzu ist es aber nöthig verschiedene Fälle zu unterscheiden.

Erstens: $\sigma = 1$. Wir fragen nach der Anzahl der Combinationen (α, γ), für welche $a\alpha^2 + 2b\alpha\gamma + c\gamma^2$ oder, da a relative Primzahl gegen 2Δ ist, für welche

$$a(a\alpha^2 + 2b\alpha\gamma + c\gamma^2) = (a\alpha + b\gamma)^2 \pm \Delta\gamma^2$$

relative Primzahl gegen 2Δ wird. Setzt man zunächst für γ irgend eine der Δ geraden Zahlen

$$0,\ 2,\ 4 \ldots (2\Delta - 2),$$

so ist erforderlich und hinreichend, dass $(a\alpha + b\gamma)^2$ und folglich $(a\alpha + b\gamma)$ relative Primzahl gegen 2Δ werde; lässt man aber α das in Bezug auf den Modulus 2Δ vollständige Restsystem

$$0,\ 1,\ 2 \ldots (2\Delta - 1)$$

durchlaufen, während γ seinen Werth behält, so durchläuft (nach §. 18) der Ausdruck $(a\alpha + b\gamma)$, weil a relative Primzahl gegen den Modulus ist, ebenfalls ein vollständiges Restsystem, und folg-

lich gehören zu jedem solchen geraden γ genau $\varphi(2\Delta)$ erlaubte Werthe von α, wo die Charakteristik φ im frühern Sinne (§. 11) gebraucht ist. Jedem der Δ ungeraden Werthe

$$1,\ 3 \ldots (2\Delta - 1)$$

von γ entsprechen ebenfalls $\varphi(2\Delta)$ erlaubte Werthe von α; dies leuchtet unmittelbar ein, wenn Δ gerade ist, weil die Forderung sich dann ebenfalls darauf reducirt, dass $(a\alpha + b\gamma)$ relative Primzahl gegen 2Δ werden muss. Ist aber Δ und also auch $\pm\Delta\gamma^2$ ungerade, so muss, da

$$(a\alpha + b\gamma)^2 \pm \Delta\gamma^2$$

ungerade und relative Primzahl gegen Δ werden soll, $(a\alpha + b\gamma)$ gerade und relative Primzahl gegen Δ werden, und folglich muss auch der Rest von $(a\alpha + b\gamma)$ in Bezug auf den Modul 2Δ gerade und relative Primzahl gegen Δ sein, und umgekehrt wird, sobald dies der Fall ist, die obige Forderung erfüllt sein. Durchläuft nun α alle seine 2Δ Werthe, so durchläuft der Rest von $(a\alpha + b\gamma)$ dieselben 2Δ Werthe; unter diesen sind die folgenden Δ Reste gerade

$$0,\ 2,\ 4 \ldots 2(\Delta - 1),$$

und unter diesen sind $\varphi(\Delta)$ relative Primzahlen gegen die ungerade Zahl Δ. Dies ist also die Anzahl der zu jedem ungeraden γ gehörenden erlaubten Werthe von α; da nun aber Δ ungerade, also relative Primzahl gegen 2 ist, so ist auch $\varphi(2\Delta) = \varphi(2)\varphi(\Delta) = \varphi(\Delta)$, und folglich haben wir in allen Fällen dieselbe Antwort: zu jedem geraden oder ungeraden γ gehören stets $\varphi(2\Delta)$ erlaubte Werthe von α; mithin existiren im Ganzen $2\Delta\varphi(2\Delta)$ erlaubte Combinationen (α, γ).

Zweitens: $\sigma = 2$; a und c gerade, b ungerade und $D \equiv 1 \pmod{4}$. Es fragt sich: für wieviele Combinationen (α, γ) ist

$$\tfrac{1}{2} a\alpha^2 + b\alpha\gamma + \tfrac{1}{2} c\gamma^2$$

ungerade und relative Primzahl gegen Δ? — Wir beschränken uns aber zunächst darauf, die Combinationen zu bestimmen, für welche dieser Werth ungerade ausfällt. Da wir den Repräsentanten (a, b, c) so gewählt haben, dass $\frac{1}{2}a$ relative Primzahl gegen 2Δ und also auch ungerade ist, so wird

$$D = b^2 - ac \equiv 1 \text{ oder } \equiv 5 \pmod{8},$$

je nachdem $\frac{1}{2}c$ gerade oder ungerade ist; im ersten Fall muss daher $\alpha(\frac{1}{2}a\alpha + b\gamma)$ ungerade, also α ungerade und γ gerade sein; im zweiten Fall muss mindestens eine der beiden Zahlen α und γ ungerade sein. Die Anzahl der erlaubten Combinationen ist hierdurch im ersten Fall auf Δ^2, im zweiten auf $3\Delta^2$ herabgedrückt.

Soll nun der Werth von $\frac{1}{2}a\alpha^2 + b\alpha\gamma + \frac{1}{2}c\gamma^2$ auch relative Primzahl gegen Δ werden, so ist erforderlich und hinreichend, dass

$$(a\alpha + b\gamma)^2 \pm \Delta\gamma^2 = 2a(\tfrac{1}{2}a\alpha^2 + b\alpha\gamma + \tfrac{1}{2}c\alpha^2)$$

oder also $(a\alpha + b\gamma)$ relative Primzahl gegen Δ werde. Im ersten Fall, wo $D \equiv 1 \pmod{8}$ ist, dürfen für γ nur gerade, für α nur ungerade Werthe gesetzt werden. Giebt man daher γ einen bestimmten der Δ Werthe

$$0,\ 2,\ 4 \ldots (2\Delta - 2)$$

und lässt dann α die sämmtlichen Δ Werthe

$$1,\ 3,\ 5 \ldots (2\Delta - 1)$$

durchlaufen, welche offenbar in Bezug auf den Modul Δ ein vollständiges Restsystem bilden, so gilt (da a relative Primzahl gegen Δ ist) dasselbe von den Δ entsprechenden Zahlen $(a\alpha + b\gamma)$, und folglich sind unter denselben $\varphi(\Delta) = \varphi(2\Delta)$ relative Primzahlen gegen Δ. Im Ganzen giebt es daher in diesem Fall $\Delta\varphi(2\Delta)$ erlaubte Combinationen (α, γ). — Im zweiten Fall, wo $D \equiv 5 \pmod{8}$ ist, und in welchem mindestens eine der beiden Zahlen α, γ ungerade sein muss, findet man auf dieselbe Weise, dass jedem geraden Werthe von γ wieder $\varphi(\Delta) = \varphi(2\Delta)$ ungerade Werthe von α entsprechen, woraus zunächst $\Delta\varphi(2\Delta)$ zulässige Combinationen entspringen; ist aber γ ungerade, und durchläuft α seine sämmtlichen 2Δ Werthe, so durchläuft der Ausdruck $(a\alpha + b\gamma)$ zweimal dasselbe vollständige Restsystem in Bezug auf den Modulus Δ; es giebt daher immer $2\varphi(\Delta) = 2\varphi(2\Delta)$ erlaubte Werthe von α, so dass aus den Δ ungeraden Werthen von γ genau $2\Delta\varphi(2\Delta)$ erlaubte Combinationen (α, γ) entspringen. Im Ganzen giebt es daher in diesem zweiten Fall $3\Delta\varphi(2\Delta)$ erlaubte Combinationen (α, γ).

Wir können die sämmtlichen Fälle so zusammenfassen: die Anzahl der Paare von zusammengehörigen arithmetischen Reihen

$$x = 2\Delta v + \alpha, \quad y = 2\Delta w + \gamma$$

welche der Bedingung I) genügen, ist

$$= \omega \cdot \Delta \varphi (2\Delta),$$

wo

$$\omega = 2, \text{ wenn } \sigma = 1$$
$$\omega = 1, \text{ wenn } \sigma = 2 \text{ und } D \equiv 1 \pmod{8}$$
$$\omega = 3, \text{ wenn } \sigma = 2 \text{ und } D \equiv 5 \pmod{8}$$

ist.

§. 95.

Wir kehren nun zu unserer Hauptgleichung zurück, der wir die Form

$$\varrho \sum \frac{1}{(ax^2 + 2bxy + cy^2)^{1+\varrho}} + \ldots = \frac{\varrho \varkappa}{\sigma^{1+\varrho}} \sum \frac{1}{n^{1+\varrho}} \sum \left(\frac{D}{n}\right) \frac{1}{n^{1+\varrho}}$$

geben, indem wir $s = 1 + \varrho$ setzen, mit ϱ multipliciren und durch $\sigma^{1+\varrho}$ dividiren; lassen wir jetzt die positive Zahl ϱ unendlich klein werden, so haben wir die Grenzwerthe der einzelnen Glieder zu bestimmen, welche sich auf der linken und rechten Seite befinden. Indem wir mit der Discussion der linken Seite beginnen, wird es wieder nothwendig, den Fall einer negativen Determinante von dem einer positiven vollständig zu trennen.

Wir nehmen daher zunächst an, die Determinante D sei *negativ* $= -\Delta$. Dann sind die Variabeln x, y in der der Form (a, b, c) entsprechenden Hauptsumme nur der Bedingung I) unterworfen, und wir haben eben gesehen, dass eine solche Hauptsumme in $\omega \Delta \varphi (2\Delta)$ Partialreihen zerfällt, welche den einzelnen zulässigen Combinationen (α, γ) entsprechen. Betrachten wir daher zunächst nur eine einzige solche Partialsumme

$$\varrho \sum \frac{1}{(ax^2 + 2bxy + cy^2)^{1+\varrho}},$$

in welcher x, y alle Werthe

$$x = 2\Delta v + \alpha, \quad y = 2\Delta w + \gamma$$

zu durchlaufen haben, die einer bestimmten zulässigen Combination (α, γ) und allen denkbaren ganzzahligen Werthen v, w entsprechen. Nach den in den Supplementen (II. §. 118) aufgestellten Principien ist der Grenzwerth des vorstehenden Productes identisch mit dem des Quotienten $T : t$, wo t eine über alle Grenzen wachsende positive Zahl und T die zugehörige Anzahl der dargestellten Zahlen $ax^2 + 2bxy + cy^2$ bedeutet, welche nicht grösser als t sind, in Zeichen, für welche

$$ax^2 + 2bxy + cy^2 \leqq t$$

oder also

$$a\left(\frac{x}{\sqrt{t}}\right)^2 + 2b\frac{x}{\sqrt{t}} \cdot \frac{y}{\sqrt{t}} + c\left(\frac{y}{\sqrt{t}}\right)^2 \leqq 1$$

ist. Dieser Grenzwerth des Quotienten $T : t$ lässt sich leicht mit Hülfe einer geometrischen Betrachtung bestimmen; setzt man nämlich

$$\frac{x}{\sqrt{t}} = \xi, \quad \frac{y}{\sqrt{t}} = \eta,$$

so ist T die Anzahl der Werthenpaare

$$\xi = \frac{2\Delta}{\sqrt{t}}v + \frac{\alpha}{\sqrt{t}}, \quad \eta = \frac{2\Delta}{\sqrt{t}}w + \frac{\gamma}{\sqrt{t}}, \tag{1}$$

für welche

$$a\xi^2 + 2b\xi\eta + c\eta^2 \leqq 1 \tag{2}$$

wird; sieht man nun ξ, η als rechtwinklige Coordinaten eines Punctes in einer Ebene an, und lässt man v und w alle ganzzahligen Werthe durchlaufen, so bilden die durch die Formeln (1) bestimmten Puncte (ξ, η) ein Gitter, welches durch die rechtwinklige Kreuzung zweier Systeme von Geraden entsteht, die den Axen parallel sind, und von denen je zwei benachbarte die constante Distanz $\delta = 2\Delta : \sqrt{t}$ haben. Die ganze Ebene wird auf diese Weise in Quadrate von dem Flächeninhalt

$$\delta^2 = \frac{4\Delta^2}{t}$$

zerlegt, deren Eckpuncte jene Puncte (ξ, η) sind; und folglich ist T die Anzahl derjenigen dieser Gitterpuncte (ξ, η), welche nicht ausserhalb der durch die Gleichung

$$a\xi^2 + 2b\xi\eta + c\eta^2 = 1 \tag{3}$$

dargestellten Curve liegen; da nun $b^2 - ac = -\varDelta$ negativ (und a positiv) ist, so ist diese Curve eine Ellipse, deren Mittelpunct mit dem Nullpunct des Coordinatensystems zusammenfällt. Nach einem ebenfalls in den Supplementen (III. §. 120) aufgestellten Hülfssatz hat folglich das Product

$$T \cdot \delta^2 = 4\varDelta^2 \cdot \frac{T}{t}$$

den Flächeninhalt A dieser Ellipse zum Grenzwerth, wenn t unendlich gross und also δ unendlich klein wird; es ist daher der gesuchte Grenzwerth

$$\lim \frac{T}{t} = \frac{A}{4\varDelta^2},$$

woraus schon folgt, dass derselbe von (α, γ) unabhängig und also für jede der $\omega\varDelta\varphi(2\varDelta)$ Partialsummen, welche unsere Hauptsumme constituiren, derselbe ist. Mithin ist der Grenzwerth dieser, der Form (a, b, c) entsprechenden, Hauptsumme

$$\varrho \sum \frac{1}{(ax^2 + 2bxy + cy^2)^{1+\varrho}}$$

gleich

$$\omega\varDelta\varphi(2\varDelta) \cdot \frac{A}{4\varDelta^2} = \frac{\omega\varphi(2\varDelta)}{4\varDelta} A,$$

wo A den Flächeninhalt der Ellipse (3) bezeichnet*). Um diesen zu bestimmen, transformire man die Gleichung der Ellipse durch Einführung solcher rechtwinkliger Coordinaten, welche mit den Hauptaxen der Ellipse zusammenfallen, wodurch sie die Form

$$a'\xi'^2 + c'\eta'^2 = 1$$

annehmen wird. Bekanntlich bleibt bei einer solchen orthogonalen Transformation die Determinante $ac - b^2$ ungeändert, so dass

---

*) Daraus, dass der Quotient $T : t$ sich einem bestimmten Grenzwerth nähert, geht zufolge des in den Supplementen (II. §. 118) aufgestellten Satzes nachträglich hervor, dass die bisher betrachteten unendlichen Reihen für jeden positiven Werth von ϱ, also für alle Werthe $s > 1$ convergiren.

$$a'c' = ac - b^2 = \Delta$$

ist; andererseits sind $\sqrt{a'}$ und $\sqrt{c'}$ die reciproken Werthe der beiden Halbaxen, und folglich ist

$$A = \frac{\pi}{\sqrt{a'c'}} = \frac{\pi}{\sqrt{\Delta}},$$

wo natürlich die Quadratwurzel *positiv* zu nehmen ist. Es ergiebt sich also das merkwürdige Resultat, dass dieser Flächeninhalt A, und folglich auch der obige Grenzwerth

$$\frac{\omega\pi\varphi(2\Delta)}{4\Delta\sqrt{\Delta}}$$

der auf die eine Form (a, b, c) bezüglichen Hauptsumme von den einzelnen Coefficienten a, b, c, und folglich von der individuellen Natur dieser Form gänzlich unabhängig ist. Denselben Grenzwerth wird daher jede andere, einer anderen Form (a', b', c') des Systems S entsprechende, Hauptsumme haben; bezeichnen wir daher mit h die Anzahl dieser einzelnen Hauptsummen auf der linken Seite unserer Gleichung, d. h. also die *Anzahl der Classen nicht äquivalenter ursprünglicher Formen der σten Art für die negative Determinante $D = -\Delta$*, so wird der Grenzwerth der ganzen linken Seite gleich

$$\frac{\omega\pi\varphi(2\Delta)}{4\Delta\sqrt{\Delta}}h.$$

§. 96.

Gehen wir nun zur rechten Seite der Gleichung über, so haben wir wieder mit Hülfe der in den Supplementen (II. §. 117) aufgestellten Principien den Grenzwerth des Productes

$$\varrho\sum\frac{1}{n^{1+\varrho}}$$

zu ermitteln, wo das Summenzeichen sich auf alle positiven ganzen Zahlen n bezieht, die relative Primzahlen gegen 2Δ sind. Bezeichnet man nun mit $\nu, \nu', \nu'' \ldots$ die $\varphi(2\Delta)$ ersten dieser Zahlen, nämlich diejenigen, welche $< 2\Delta$ sind, so kann man die vorstehende Summe in $\varphi(2\Delta)$ Partialsummen von der Form

$$\varrho \left\{ \frac{1}{\nu^{1+\varrho}} + \frac{1}{(\nu + 2\Delta)^{1+\varrho}} + \frac{1}{(\nu + 4\Delta)^{1+\varrho}} + \frac{1}{(\nu + 6\Delta)^{1+\varrho}} + \cdots \right\}$$

zerlegen, in welcher die unter dem Exponenten $(1 + \varrho)$ stehenden Zahlen jedesmal eine arithmetische Reihe von der Differenz 2Δ bilden; da nun nach dem in den Supplementen behandelten speciellen Fall der Grenzwerth einer solchen Partialreihe

$$= \frac{1}{2\Delta}$$

und also unabhängig von ν ist, so wird der Grenzwerth der ganzen Summe

$$= \frac{\varphi(2\Delta)}{2\Delta},$$

und mithin wird der Grenzwerth der ganzen rechten Seite der Hauptgleichung

$$\frac{\varkappa \varphi(2\Delta)}{\sigma \cdot 2\Delta} \lim \Sigma \left(\frac{D}{n}\right) \frac{1}{n^{1+\varrho}}.$$

Da aber beide Seiten für jeden Werth von $s > 1$, d. h. für jeden positiven Werth von ϱ identisch sind, und da sie folglich, wenn überhaupt einen, nothwendig denselben Grenzwerth haben müssen, so ergiebt sich aus der Vergleichung, indem wir $D = -\Delta$ restituiren,

$$h = \frac{\varkappa}{\sigma \omega} \frac{2}{\pi} \sqrt{-D} \cdot \lim \Sigma \left(\frac{D}{n}\right) \frac{1}{n^{1+\varrho}}$$

als Ausdruck für die Classenanzahl der ursprünglichen Formen σter Art (mit positiven äussern Coefficienten) für eine *negative* Determinante D; hierin ist ferner

$\varkappa = 4$, wenn $D = -1$,
$\varkappa = 6$, wenn $D = -3$ und $\sigma = 2$,
$\varkappa = 2$ in den übrigen Fällen;

und

$\omega = 2$, wenn $\sigma = 1$,
$\omega = 1$, wenn $\sigma = 2$ und $D \equiv 1 \pmod{8}$,
$\omega = 3$, wenn $\sigma = 2$ und $D \equiv 5 \pmod{8}$.

§. 97.

Für Formen der ersten Art erhalten wir daher, indem wir $\sigma = 1$, $\varkappa = 2$ und $\omega = 2$ setzen,

$$h = \frac{2}{\pi}\sqrt{-D} \cdot \lim \Sigma \left(\frac{D}{n}\right)\frac{1}{n^{1+\varrho}},$$

mit Ausnahme des einzigen Falles $D = -1$, in welchem $\varkappa$ nicht $= 2$, sondern $= 4$ ist, und folglich

$$h = \frac{4}{\pi} \lim \Sigma \frac{(-1)^{\frac{1}{2}(n-1)}}{n^{1+\varrho}}$$

wird; es wird später (§§. 101, 105) allgemein gezeigt werden, dass

$$\lim \Sigma \left(\frac{D}{n}\right)\frac{1}{n^{1+\varrho}} = \Sigma \left(\frac{D}{n}\right)\frac{1}{n}$$

ist, vorausgesetzt, dass auf der rechten Seite die Glieder ihrer Grösse nach geordnet werden; in dem speciellen Fall $D = -1$ wird daher

$$h = \frac{4}{\pi}\left(1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \cdots\right) = 1,$$

da der Werth der in der Parenthese befindlichen unendlichen Reihe von *Leibnitz* bekanntlich $= \frac{1}{4}\pi$ ist; hierin liegt also eine Bestätigung unserer Principien, da in der That für die Determinante $D = -1$ nur eine einzige Classe von Formen (mit positiven äussern Coefficienten) existirt.

Wir wollen nun mit der vorstehenden Formel für die Classenanzahl h der Formen der ersten Art die für die Anzahl h' der Formen der zweiten Art vergleichen. Wir unterscheiden zu dem Zweck die beiden Fälle, in welchen $D \equiv 1$ oder $D \equiv 5 \pmod{8}$ ist. Im ersten Fall ist $\varkappa = 2$ und $\omega = 1$, folglich

$$h' = \frac{2}{\pi}\sqrt{-D} \cdot \lim \Sigma \left(\frac{D}{n}\right)\frac{1}{n^{1+\varrho}} = h;$$

im zweiten Fall dagegen ist $\omega = 3$ und $\varkappa = 2$, also

$$h' = \frac{1}{3} \cdot \frac{2}{\pi}\sqrt{-D} \cdot \lim \Sigma \left(\frac{D}{n}\right)\frac{1}{n^{1+\varrho}} = \frac{1}{3}h,$$

ausgenommen den einzigen Fall $D = -3$, in welchem $\varkappa$ nicht $= 2$, sondern $= 6$, und folglich wieder

$$h' = h$$

ist. Wir können daher so zusammenfassen: es ist

$$h' = h, \text{ wenn } D \equiv 1 \pmod{8}, \text{ und für } D = -3;$$
$$h' = \tfrac{1}{3} h, \text{ wenn } D \equiv 5 \pmod{8}, \text{ ausgenommen } D = -3.$$

Diese Beziehungen zwischen der Anzahl der Formen der ersten und der zweiten Art hat schon *Gauss* gefunden, aber auf einem ganz andern Wege.*)

§. 98.

Wir haben nun dieselbe Untersuchung für den Fall einer *positiven* Determinante $D = \Delta$ zu wiederholen. Betrachten wir zunächst die linke Seite, so zerlegen wir wieder jede auf eine bestimmte Form (a, b, c) bezügliche Hauptsumme in $\omega \Delta \varphi(2\Delta)$ Partialsummen von der Form

$$\varrho \sum \frac{1}{(ax^2 + 2bxy + cy^2)^{1+\varrho}},$$

in deren jeder die Summationsbuchstaben alle Werthenpaare

$$x = 2\Delta v + \alpha, \quad y = 2\Delta w + \gamma \tag{1}$$

zu durchlaufen haben, die einer bestimmten Combination (α, γ) und allen ganzzahligen Werthen v, w entsprechen; jetzt aber treten ausserdem noch die Isolirungsbedingungen II) hinzu, denen gemäss

$$y \geqq 0, \quad ax + by > \frac{T}{U} y \tag{2}$$

sein soll. Diese letztern Bedingungen haben, wie wir schon früher gesehen haben (§. 87), zur Folge, dass

$$ax + (b + \sqrt{D})y, \quad ax + (b - \sqrt{D})\, y,$$

und also auch

*) *Disquisitiones Arithmeticae* art. 256. VI.

$$ax^2 + 2bxy + cy^2$$

positive Zahlen sind, und wir können daher wieder die in den Supplementen aufgestellten Principien anwenden; bezeichnen wir mit t einen beliebigen positiven Werth und mit T die Anzahl derjenigen in den Reihen (1) enthaltenen und zugleich den Bedingungen (2) genügenden Werthenpaare x, y, für welche

$$ax^2 + 2bxy + cy^2 \leqq t \tag{3}$$

ist, so haben wir nur den Grenzwerth des Quotienten $T:t$ für unbegrenzt wachsende Werthe von t zu bestimmen, um dadurch zugleich den Grenzwerth der obigen Partialsumme zu finden, welche der einen Combination (α, γ) entspricht. Setzen wir wieder (indem wir $\sqrt{t}$ positiv nehmen)

$$\xi = \frac{x}{\sqrt{t}}, \quad \eta = \frac{y}{\sqrt{t}},$$

und sehen wir ξ, η als rechtwinklige Coordinaten eines Punctes einer Ebene an, so ist T die Anzahl derjenigen in der Doppelreihe

$$\xi = \frac{2\varDelta}{\sqrt{t}} v + \frac{\alpha}{\sqrt{t}}, \quad \eta = \frac{2\varDelta}{\sqrt{t}} w + \frac{\gamma}{\sqrt{t}}$$

enthaltenen Gitterpuncte, welche den drei Ungleichheiten

$$\eta \geqq 0, \quad \xi > \frac{1}{a}\left(\frac{T}{U} - b\right)\eta,$$
$$a\xi^2 + 2b\xi\eta + c\eta^2 \leqq 1$$

Genüge leisten, d. h. welche innerhalb eines Stückes der $\xi\eta$-Ebene liegen, das zum Theil durch die Axe der ξ, zum Theil durch eine durch den Nullpunct gehende Gerade, und endlich durch eine Hyperbel begrenzt wird, die den Nullpunct zum Mittelpuncte hat. Bezeichnen wir mit B den Flächeninhalt dieses Stückes der $\xi\eta$-Ebene, so wird nach den in den Supplementen aufgestellten Principien, wenn t unendlich gross und also die Kante $\delta = 2\varDelta : \sqrt{t}$ der Gitterquadrate unendlich klein wird,

$$\lim T \cdot \delta^2 = 4\varDelta^2 \cdot \lim \frac{T}{t} = B,$$

also

$$\lim \frac{T}{t} = \frac{B}{4\varDelta^2}$$

sein. Da dieser Grenzwerth zugleich der Grenzwerth der Partialsumme ist, welche sich auf die eine Combination (α, γ) bezieht, so wird, da hierin die Werthe α, γ ganz herausgefallen sind, jede der $\omega \varDelta \varphi(2\varDelta)$ Partialsummen, welche den verschiedenen Combinationen (α, γ) entsprechen und welche zusammen die auf die Form (a, b, c) bezügliche Hauptsumme constituiren, denselben Grenzwerth haben; und mithin wird

$$\frac{\omega \varphi(2\varDelta)}{4\varDelta} B$$

der Grenzwerth der ganzen Hauptsumme

$$\varrho \sum \frac{1}{(ax^2 + 2bxy + cy^2)^{1+\varrho}}$$

sein. Um nun den Flächeninhalt B des durch die drei obigen Ungleichheiten definirten Hyperbelsectors zu finden, wird man am besten Polarcoordinaten r, φ einführen, indem man

$$\xi = r \cos\varphi, \quad \eta = r \sin\varphi$$

setzt, wo, wie gewöhnlich, r stets positiv und φ zwischen 0 und 2π genommen werden soll, was hinreicht, um jeden Punct (ξ, η) der Ebene einmal und nur einmal zu erzeugen. Durch diese Transformation verwandeln sich die frühern Grenzbedingungen in folgende:

$$\sin\varphi \geqq 0; \quad \text{cotang}\,\varphi > \frac{1}{a}\left(\frac{T}{U} - b\right);$$

$$r^2 (a \cos\varphi^2 + 2b \cos\varphi \sin\varphi + c \sin\varphi^2) \leqq 1,$$

und wir wiederholen die frühere Bemerkung, dass für jeden den beiden ersten Bedingungen genügenden Winkel φ die Grössen

$$a \cos\varphi + (b + \sqrt{D}) \sin\varphi, \quad a \cos\varphi + (b - \sqrt{D}) \sin\varphi,$$
$$a \cos\varphi^2 + 2b \cos\varphi \sin\varphi + c \sin\varphi^2$$

positiv sind, so dass also innerhalb des durch diese beiden ersten Bedingungen begrenzten Winkelraums keine Asymptote, sondern nur ein endliches Stück der Hyperbel liegt, woraus schon folgt, dass der entsprechende Sector jedenfalls einen endlichen Werth hat *). Dieser wird bekanntlich durch die Formel

*) Hieraus folgt wieder nachträglich die Convergenz der bisher betrachteten Reihen für jeden positiven Werth von ϱ, d. h. für jeden Werth von $s > 1$.

$$B = \int\int r dr d\varphi = \tfrac{1}{2}\int r^2 d\varphi$$

gefunden, wo nun in dem einfachen Integral rechts für r^2 der in der Peripherie der Hyperbel geltende Werth

$$r^2 = \frac{1}{a\cos\varphi^2 + 2b\cos\varphi\sin\varphi + c\sin\varphi^2}$$

$$= \frac{a}{2\sqrt{D}}\left\{\frac{1}{a\,\text{cotang}\,\varphi + b - \sqrt{D}} - \frac{1}{a\,\text{cotang}\,\varphi + b + \sqrt{D}}\right\}\frac{1}{\sin\varphi^2}$$

zu setzen ist; wir erhalten daher, indem wir cotang φ als neue Variabele betrachten, und

$$\frac{d\varphi}{\sin\varphi^2} = -\,d\,\text{cotang}\,\varphi$$

setzen, das unbestimmte Integral

$$\frac{1}{2}\int r^2 d\varphi =$$

$$\frac{1}{4\sqrt{D}}\int\frac{a\,d\,\text{cotang}\,\varphi}{a\,\text{cotang}\,\varphi + b + \sqrt{D}} - \frac{1}{4\sqrt{D}}\int\frac{a\,d\,\text{cotang}\,\varphi}{a\,\text{cotang}\,\varphi + b - \sqrt{D}}$$

$$= \frac{1}{4\sqrt{D}}\log\frac{a\,\text{cotang}\,\varphi + b + \sqrt{D}}{a\,\text{cotang}\,\varphi + b - \sqrt{D}};$$

diese Integration ist aber auszudehnen über alle Werthe von φ, welche einen positiven Sinus haben, also von $\varphi = 0$ ab bis zu dem Werth, wo $U\,(a\,\text{cotang}\,\varphi + b) = T$ wird; dieser Endwerth von φ ist durch die Bedingung, dass $\sin\varphi$ positiv sein soll, vollständig bestimmt, und wir haben schon oben darauf hingewiesen, dass innerhalb dieses ganzen Winkelraums die beiden Grössen

$$a\,\text{cotang}\,\varphi + b + \sqrt{D},\quad a\,\text{cotang}\,\varphi + b - \sqrt{D}$$

stets das positive Zeichen behalten, so dass das obige unbestimmte Integral eine stetige reelle Function von φ ist, woraus folgt, dass wir nur die beiden Grenzen in dasselbe einzusetzen haben. Auf diese Weise erhalten wir

$$B = \frac{1}{4\sqrt{D}}\log\frac{T + U\sqrt{D}}{T - U\sqrt{D}} = \frac{1}{2\sqrt{D}}\log\frac{T + U\sqrt{D}}{\sigma}.$$

Der Grenzwerth der auf die Form (a, b, c) bezüglichen Haupt-

summe wird daher, wenn man statt Δ wieder D schreibt, gleich

$$\frac{\omega\varphi(2D)}{8D\sqrt{D}}\log\frac{T+U\sqrt{D}}{\sigma},$$

worin, wie früher, T, U die beiden kleinsten der unbestimmten Gleichung $T^2 - DU^2 = \sigma^2$ genügenden positiven Zahlen bedeuten. Mithin zeigt sich auch hier, wie früher bei den Formen von negativer Determinante, dass der Grenzwerth einer auf eine einzelne Form (a, b, c) des Systems S bezüglichen Hauptsumme nur von der Determinante D (und der Art σ), dagegen gar nicht von dem individuellen Charakter der Form abhängt, dass er also für alle diese Formen derselbe ist. Bezeichnen wir wieder mit h die Anzahl aller in S enthaltenen Formen, d. h. die *Anzahl aller Classen ursprünglicher Formen σter Art für die positive Determinante D*, so ist daher

$$h\frac{\omega\varphi(2D)}{8D\sqrt{D}}\log\frac{T+U\sqrt{D}}{\sigma}$$

der Grenzwerth, welchem sich für unendlich abnehmende positive Werthe von ϱ die linke Seite unserer Hauptgleichung nähert. Auf der rechten Seite ist $\varkappa = 1$, ferner ebenso wie früher bei Formen von negativer Determinante

$$\lim\varrho\sum\frac{1}{n^{1+\varrho}} = \frac{\varphi(2\Delta)}{2\Delta} = \frac{\varphi(2D)}{2D},$$

und folglich erhalten wir durch Vergleichung beider Seiten der Hauptgleichung das Resultat

$$h = \frac{1}{\sigma\omega}\cdot\frac{4\sqrt{D}}{\log\frac{T+U\sqrt{D}}{\sigma}}\cdot\lim\sum\left(\frac{D}{n}\right)\frac{1}{n^{1+\varrho}}.$$

§. 99.

Für Formen der ersten Art ist $\sigma = 1$ und $\omega = 2$; hieraus folgt für die Anzahl der Classen ursprünglicher Formen erster Art der Ausdruck

$$h = \frac{2\sqrt{D}}{\log(T+U\sqrt{D})}\cdot\lim\sum\left(\frac{D}{n}\right)\frac{1}{n^{1+\varrho}},$$

wo T, U die kleinsten der Gleichung

$$T^2 - DU^2 = 1$$

genügenden positiven ganzen Zahlen bedeuten. Ist ferner $D \equiv 1$ (mod. 4), so existiren auch Formen der zweiten Art, deren Anzahl wir mit h' bezeichnen wollen; es ist dann $\sigma = 2$ und $\omega = 1$ oder $= 3$ zu setzen, je nachdem $D \equiv 1$ (mod. 8) oder $\equiv 5$ (mod. 8) ist; wir erhalten daher, wenn wir zur Unterscheidung mit T', U' die kleinsten der unbestimmten Gleichung

$$T'^2 - DU'^2 = 4$$

genügenden ganzen positiven Zahlen bezeichnen,

$$h' = \frac{1}{\omega} \cdot \frac{2\sqrt{D}}{\log \frac{1}{2}(T' + U'\sqrt{D})} \cdot \lim \Sigma\left(\frac{D}{n}\right)\frac{1}{n^{1+\varrho}}.$$

Nun ist einleuchtend, dass jede Auflösung (t, u) der Gleichung $t^2 - Du^2 = 1$ durch Verdoppelung eine Auflösung $(t' = 2t, u' = 2u)$ der Gleichung $t'^2 - Du'^2 = 4$ giebt, und umgekehrt, dass man durch Halbirung jeder *geraden* Auflösung (t', u') der letztern eine Auflösung (t, u) der erstern erhält. Hieraus folgt unmittelbar, dass $(t' = 2T, u' = 2U)$ jedenfalls die kleinste gerade Auflösung der Gleichung $t'^2 - Du'^2 = 4$ ist. Ist nun zunächst $D \equiv 1$ (mod. 8), so kann diese Gleichung überhaupt nur gerade Auflösungen haben; denn wäre eine der beiden Zahlen t', u' und folglich auch die andere ungerade, so wäre die linke Seite durch 8 theilbar, während sie doch $= 4$ sein soll; in diesem Fall ist daher

$$T' = 2T,\ U' = 2U,\ \frac{T' + U'\sqrt{D}}{2} = T + U\sqrt{D},$$

und da ausserdem $\omega = 1$ ist, so ergiebt sich

$$h' = h, \text{ wenn } D \equiv 1 \pmod{8}.$$

Im andern Fall $D \equiv 5$ (mod. 8) kann die Regel nicht so bestimmt ausgesprochen werden, indem bei manchen dieser Determinanten die kleinste Auflösung (T', U') wieder eine gerade, bei andern aber eine ungerade ist. Im ersten dieser beiden Fälle ist dann wieder $T' = 2T$, $U' = 2U$ und folglich, da $\omega = 3$ ist,

$$h' = \tfrac{1}{3}h, \text{ wenn } D \equiv 5 \pmod{8} \text{ und } T', U' \text{ gerade;}$$

es giebt unterhalb 200 nur 5 Determinanten, nämlich 37, 101, 141, 189, 197, für welche dieser Fall eintritt.

Im zweiten Falle, wenn T', U' ungerade sind, haben wir unter allen positiven Auflösungen (t', u'), welche (§. 85) aus der Formel

$$\frac{t' + u'\sqrt{D}}{2} = \left(\frac{T' + U'\sqrt{D}}{2}\right)^n$$

für positive Werthe von n entspringen, die kleinste gerade aufzusuchen. Versuchen wir daher die nächst grössere Auflösung, welche dem Exponenten $n = 2$ entspricht, so erhalten wir

$$t' = \frac{T'^2 + DU'^2}{2}, \quad u' = T'U';$$

da u' offenbar ungerade ist, so gehen wir zu dem folgenden Exponenten $n = 3$ über, um die nächst grössere Auflösung zu prüfen; da finden wir

$$t' = \frac{T'^3 + 3DT'U'^2}{4} = T' \frac{T'^2 + 3DU'^2}{4},$$

und da

$$T'^2 \equiv U'^2 \equiv 1 \pmod{8}, \quad 3D \equiv -1 \pmod{8}$$

ist, so folgt, dass t' und folglich auch u' gerade Zahlen werden, und also $t' = 2T$, $u' = 2U$ ist. Wir haben daher in diesem Fall

$$T + U\sqrt{D} = \left(\frac{T' + U'\sqrt{D}}{2}\right)^3$$

und

$$\log \frac{T + U'\sqrt{D}}{2} = \tfrac{1}{3} \log (T + U\sqrt{D});$$

berücksichtigt man ferner, dass $\omega = 3$ ist, so ergiebt sich die Relation

$$h' = h, \text{ wenn } D \equiv 5 \pmod{8}, \text{ und } T', U' \text{ ungerade.}$$

Auch für positive Determinanten hat *Gauss* *) ebenfalls die

---

*) *Disquisitiones Arithmeticae* art. 256. VI.

Relationen zwischen den Anzahlen der Formen der ersten und zweiten Art aufgestellt, für den letzten Fall aber, in welchem $D \equiv 5 \pmod{8}$ ist, in ganz anderer Form; er zeigt nämlich, dass die drei ursprünglichen Formen

$$(1,\ 0,\ -D),\ \left(4,\ 1,\ \frac{1-D}{4}\right),\ \left(4,\ 3,\ \frac{9-D}{4}\right)$$

entweder alle äquivalent sind, oder drei verschiedenen Classen angehören; und je nachdem das Erstere oder Letztere eintritt, ist $h' = h$ oder $h' = \frac{1}{3} h$.

§. 100.

Nachdem wir im Vorhergehenden für alle Fälle gezeigt haben, wie die Classenanzahl der Formen zweiter Art aus der der Formen erster Art gefunden werden kann, beschränken wir die fernere Untersuchung lediglich auf die Bestimmung der letztern. Bevor wir aber dazu übergehen, können wir eine weitere Zurückführung unserer Aufgabe vornehmen, indem wir zeigen, dass man nur solche Determinanten D zu betrachten braucht, welche durch keine Quadratzahl (ausser 1) theilbar sind.

Ist D' eine beliebige Determinante, so kann man immer $D' = D S^2$ setzen, wo S^2 das grösste in D' aufgehende Quadrat, und also D ein Product aus lauter ungleichen Primzahlen (oder auch $= -1$) ist, welches dem Zeichen nach mit D' übereinstimmt; dann lässt sich die Classenanzahl der Formen von der Determinante D' auf die der Formen von der Determinante D zurückführen. Bezeichnen wir alle auf die Determinante D' bezüglichen Grössen durch beigesetzte Accente, so wollen wir zunächst die beiden Summen

$$\Sigma \left(\frac{D}{n}\right) \frac{1}{n^s} \text{ und } \Sigma \left(\frac{D'}{n'}\right) \frac{1}{n'^s}$$

mit einander vergleichen, in welchen wir der Bequemlichkeit halber s statt $1 + \varrho$ geschrieben haben. In der zweiten muss der Buchstabe n' alle positiven Zahlen durchlaufen, welche relative Primzahlen gegen $2D'$ sind. Bezeichnen wir mit q' alle positiven ungeraden nicht in D' aufgehenden, und, wie früher, mit q alle

positiven ungeraden nicht in D aufgehenden Primzahlen, so ist, wie wir früher gesehen haben,

$$\Sigma \left(\frac{D}{n}\right) \frac{1}{n^s} = \Pi \frac{1}{1 - \left(\frac{D}{q}\right) \frac{1}{q^s}}$$

und natürlich ebenso

$$\Sigma \left(\frac{D'}{n'}\right) \frac{1}{n'^s} = \Pi \frac{1}{1 - \left(\frac{D'}{q'}\right) \frac{1}{q'^s}} \cdot$$

Offenbar bildet nun das System der Primzahlen q' nur einen Theil der Primzahlen q, denn eine in $D' = DS^2$ nicht aufgehende Primzahl q' geht auch nicht in D auf und ist folglich eine der Primzahlen q. Das System der Primzahlen q besteht daher aus dem der Primzahlen q' und aus solchen ungeraden Primzahlen r, welche nicht in D, wohl aber in D', also auch in S aufgehen, und deren Anzahl offenbar endlich ist. Das auf die Determinante D bezügliche unendliche Product wird sich daher in folgender Weise zerlegen

$$\Pi \frac{1}{1 - \left(\frac{D}{q}\right) \frac{1}{q^s}} = \Pi \frac{1}{1 - \left(\frac{D}{q'}\right) \frac{1}{q'^s}} \cdot \Pi \frac{1}{1 - \left(\frac{D}{r}\right) \frac{1}{r^s}};$$

da nun ferner $D' = DS^2$ und folglich

$$\left(\frac{D'}{q'}\right) = \left(\frac{DS^2}{q'}\right) = \left(\frac{D}{q'}\right)$$

ist, so erhalten wir, indem wir statt der beiden unendlichen Producte wieder die unendlichen Reihen aufschreiben, das Resultat

$$\Sigma \left(\frac{D}{n}\right) \frac{1}{n^s} = \Sigma \left(\frac{D'}{n'}\right) \frac{1}{n'^s} \cdot \Pi \frac{1}{1 - \left(\frac{D}{r}\right) \frac{1}{r^s}}$$

und hieraus

$$\lim \Sigma \left(\frac{D'}{n'}\right) \frac{1}{n'^{1+\varrho}} = \Pi \left(1 - \left(\frac{D}{r}\right) \frac{1}{r}\right) \lim \Sigma \left(\frac{D}{n}\right) \frac{1}{n^{1+\varrho}},$$

worin also das Productzeichen sich auf alle ungeraden in S, aber nicht in D aufgehenden Primzahlen r bezieht.

Nachdem wir so für positive wie negative Determinanten das Verhältniss zwischen den beiden analogen Grenzwerthen bestimmt haben, die als Factoren in den Classenanzahlen h und h' für die Determinanten D und D' auftreten, müssen wir wieder die beiden Hauptfälle von einander trennen.

Ist zunächst D' und folglich auch D *negativ*, so haben wir (da wir uns auf Formen der ersten Art beschränken)

$$h = \frac{2\sqrt{-D}}{\pi} \lim \Sigma \left(\frac{D}{n}\right) \frac{1}{n^{1+\varrho}},$$

den einzigen Fall ausgenommen, in welchem $D = -1$. Ebenso ist

$$h' = \frac{2\sqrt{-D'}}{\pi} \lim \Sigma \left(\frac{D'}{n'}\right) \frac{1}{n'^{1+\varrho}}.$$

Mit Ausnahme des Falles $D = -1$ ist daher, mit Rücksicht auf das eben gefundene Verhältniss der beiden Grenzwerthe der unendlichen Reihen,

$$h' = h \times S \cdot \Pi \left(1 - \left(\frac{D}{r}\right) \frac{1}{r}\right);$$

ist aber $D = -1$, also $\varkappa = 4$, $h = 1$, und $D' = -S^2$ nicht ebenfalls $= -1$, also $S > 1$, so ist die Classenanzahl für eine solche Determinante D' gleich

$$\tfrac{1}{2} S \, \Pi \left(1 - \frac{(-1)^{\frac{1}{2}(r-1)}}{r}\right).$$

Für *positive* Determinanten haben wir folgende Formeln erhalten:

$$h = \frac{2\sqrt{D}}{\log(T + U\sqrt{D})} \lim \Sigma \left(\frac{D}{n}\right) \frac{1}{n^{1+\varrho}}$$

$$h' = \frac{2\sqrt{D'}}{\log(T' + U'\sqrt{D'})} \lim \Sigma \left(\frac{D'}{n'}\right) \frac{1}{n'^{1+\varrho}}$$

wo T', U' die kleinsten positiven Zahlen bedeuten, die der Gleichung $T'^2 - D'U'^2 = 1$ genügen; hieraus ergiebt sich

$$h' = h \frac{\log(T + U\sqrt{D})}{\log(T' + U'\sqrt{D'})} \times S \cdot \Pi\left(1 - \left(\frac{D}{r}\right)\frac{1}{r}\right),$$

und es kommt nur noch darauf an, das Verhältniss der beiden Logarithmen in rationaler Form anzugeben. Offenbar liefert nun jede Lösung (t', u') der Gleichung

$$t'^2 - D'u'^2 = 1, \quad \text{d. h. } t'^2 - DS^2u'^2 = 1$$

eine Lösung der Gleichung

$$t^2 - Du^2 = 1,$$

in welcher

$$t = t', \quad u = Su',$$

also das zweite Element u durch S theilbar ist; und umgekehrt, sobald in der Lösung (t, u) das zweite Element u durch S theilbar ist, so erhält man hieraus eine Lösung der erstern. Hieraus folgt, dass die beiden Zahlen

$$t = T', \quad u = SU'$$

die kleinste positive Lösung der zweiten Gleichung bilden, in welcher das zweite Element durch S theilbar ist; man kann daher

$$T' + SU'\sqrt{D} = T' + U'\sqrt{D'} = (T + U\sqrt{D})^\lambda$$

setzen, wo λ der kleinste positive ganze Exponent ist, für welchen der irrationale Bestandtheil der Potenz einen durch S theilbaren Coefficienten erhält; und dann ist

$$h' = h \times \frac{1}{\lambda} \cdot S \cdot \Pi\left(1 - \left(\frac{D}{r}\right)\frac{1}{r}\right).$$

Setzt man, wie früher,

$$(T + U\sqrt{D})^\nu = t_\nu + u_\nu\sqrt{D},$$

so lässt sich der Werth von λ unmittelbar angeben, wenn für jede einzelne in S aufgehende Primzahl p die kleinste Zahl ν bekannt ist, für welche u_ν durch p theilbar, und zugleich die höchste Potenz von p gegeben ist, welche dann in u_ν aufgeht*); doch

*) *Dirichlet*: *Ueber eine Eigenschaft der quadratischen Formen von positiver Determinante* (Crelle's Journal LIII).

gehen wir hierauf nicht weiter ein, da der Hauptzweck, das Verhältniss zwischen den Classenanzahlen h und h' für die Determinanten D und $D' = DS^2$ zu finden, erreicht ist.

Dieselbe Aufgabe ist, wenigstens für negative Determinanten, auch schon von *Gauss* gelöst *).

§. 101.

In Folge der vorhergehenden Untersuchungen können wir uns auf den Fall beschränken, in welchem die Determinante D durch kein Quadrat ausser 1 theilbar ist, und es bleibt nur noch übrig, den Grenzwerth der unendlichen Reihe

$$\Sigma \left(\frac{D}{n}\right) \frac{1}{n^{1+\varrho}}$$

für unendlich abnehmende positive Werthe von ϱ wirklich zu bestimmen. Bezeichnet man mit $p', p'', p''' \ldots$ die sämmtlichen *positiven ungeraden* Primzahlen, welche in D aufgehen, und mit P ihr Product, so ist

$$\text{entweder } D = \pm P, \text{ oder } D = \pm 2P;$$

in den Fällen $D = -1$ und $D = \pm 2$ ist $P = 1$ zu setzen.

Um nun die verschiedenen Fälle bequem zusammenfassen zu können, führen wir zwei positive oder negative Einheiten δ und ε ein; wir setzen nämlich $\delta = +1$ oder $= -1$, je nachdem $\pm P \equiv 1$ oder $\equiv -1$ (mod. 4), und ähnlich $\varepsilon = +1$ oder $= -1$, je nachdem D ungerade oder gerade ist. Wir haben also die folgenden vier Fälle:

$$\begin{aligned}
D &= \pm P \equiv 1 \pmod{4}, & \delta &= +1, & \varepsilon &= +1;\\
D &= \pm P \equiv 3 \pmod{4}, & \delta &= -1, & \varepsilon &= +1;\\
D &= \pm 2P \equiv 2 \pmod{8}, & \delta &= +1, & \varepsilon &= -1;\\
D &= \pm 2P \equiv 6 \pmod{8}, & \delta &= -1, & \varepsilon &= -1.
\end{aligned}$$

Man überzeugt sich leicht, dass in allen Fällen zufolge des verallgemeinerten Reciprocitätssatzes (§. 46)

*) *Disquisitiones Arithmeticae* art. 256. V. Die obigen Sätze sind auf anderm Wege auch von *Lipschitz* bewiesen (Crelle's Journal LIII).

$$\left(\frac{D}{n}\right) = \delta^{\frac{1}{2}(n-1)} \varepsilon^{\frac{1}{8}(n^2-1)} \left(\frac{n}{P}\right)$$

ist. Schreiben wir ferner s statt $1 + \varrho$, so haben wir den Grenzwerth der unendlichen Reihe

$$\Sigma\ \delta^{\frac{1}{2}(n-1)} \varepsilon^{\frac{1}{8}(n^2-1)} \left(\frac{n}{P}\right) \frac{1}{n^s}$$

zu untersuchen für den Fall, dass der unechte Bruch s sich der Einheit unbegrenzt nähert. So lange $s > 1$ bleibt, ist diese Reihe immer convergent, und zwar ist ihre Summe durchaus unabhängig von der Ordnung, in welcher man ihre Glieder auf einander folgen lässt; ist aber $s = 1$, so gehört diese Reihe zu der Classe derjenigen, in welcher die Summe der positiven Glieder für sich, so wie die der negativen Glieder für sich genommen unendlich gross ist. Da nun unter der Summe einer unendlichen convergirenden Reihe stets der Grenzwerth verstanden wird, welchem sich die Summe ihrer *ersten* n Glieder nähert, wenn die Gliederanzahl n unbegrenzt wächst, so sieht man leicht ein, dass bei einer unendlichen Reihe von dieser eigenthümlichen Beschaffenheit erst dann von ihrer Convergenz und von ihrer Summe die Rede sein kann, nachdem ihre sämmtlichen Glieder in eine bestimmte *Ordnung* gebracht sind, nach welcher eines auf das andere folgt; denn die Summe, wenn sie überhaupt existirt, hängt wesentlich von der Compensation ab, welche zwischen den für sich allein unendlich wachsenden positiven und negativen Bestandtheilen gerade durch diese Anordnung der Glieder hervorgebracht wird. Eine solche unendliche Reihe hat daher ganz verschiedene Summen, je nach der verschiedenen Anordnung der Glieder. Aber gesetzt auch, dies wäre gar nicht der Fall, sondern die Reihe hätte auch für den Werth $s = 1$ einen vollständig bestimmten Werth, so würde sich immer noch fragen, ob dieser Werth auch der Grenzwerth ist, welchem sich der Werth der Reihe unendlich nähert, wenn s sich der Einheit unendlich nähert, d. h. es würde sich fragen, ob der Werth der unendlichen Reihe sich an der Stelle $s = 1$ *stetig* mit s ändert.

Um über alle diese Zweifel zu entscheiden, betrachten wir folgende allgemeinere Reihe

$$\frac{\alpha_1}{1^s} + \frac{\alpha_2}{2^s} + \frac{\alpha_3}{3^s} + \cdots + \frac{\alpha_m}{m^s} + \cdots$$

unter der einzigen Voraussetzung, dass die Summe

$$\beta_n = \alpha_1 + \alpha_2 + \cdots + \alpha_n$$

ihrem absoluten Werth nach eine bestimmte endliche Grösse C nie überschreitet, wie gross auch n genommen werden mag. Dann lässt sich zeigen, dass die so angeordnete unendliche Reihe für jeden *positiven* Werth des Exponenten s (excl. $s = 0$) convergirt, und für alle diese Werthe von s zugleich eine stetige Function von s ist.

Zu diesem Zweck vergleichen wir die vorstehende Reihe mit der folgenden

$$\beta_1\left(\frac{1}{1^s} - \frac{1}{2^s}\right) + \beta_2\left(\frac{1}{2^s} - \frac{1}{3^s}\right) + \beta_3\left(\frac{1}{3^s} - \frac{1}{4^s}\right) + \cdots$$

Die Summen der ersten n Glieder der erstern und letztern Reihe unterscheiden sich von einander nur um

$$\frac{\beta_n}{(n+1)^s};$$

da nun der Voraussetzung nach β_n seinem absoluten Werth nach stets unterhalb der endlichen Grösse C bleibt, und s positiv ist, so wird dieser Unterschied mit unbegrenzt wachsendem n unendlich klein werden. Nähert sich daher die Summe der ersten n Glieder der einen Reihe einem bestimmten Grenzwerth, d. h. convergirt die eine Reihe, so ist dies auch mit der andern der Fall, und zwar hat sie dieselbe Summe. Wir brauchen daher die obigen Behauptungen nur für die letztere Reihe zu beweisen; dazu betrachten wir die Summe von beliebig vielen Gliedern, welche auf die ersten n Glieder folgen:

$$\beta_{n+1}\left(\frac{1}{(n+1)^s} - \frac{1}{(n+2)^s}\right) + \cdots$$
$$+ \beta_{n+m}\left(\frac{1}{(n+m)^s} - \frac{1}{(n+m+1)^s}\right);$$

da die Differenzen

$$\frac{1}{(n+1)^s} - \frac{1}{(n+2)^s},\quad \frac{1}{(n+2)^s} - \frac{1}{(n+3)^s} \cdots$$

sämmtlich positiv sind, und ihre Factoren

$$\beta_{n+1},\quad \beta_{n+2} \;\cdot\;\cdot\;\cdot$$

absolut genommen sämmtlich kleiner als C sind, so ist die Summe dieser m Glieder absolut genommen auch kleiner als das Product aus C und der Summe jener m Differenzen, d. h. kleiner als

$$C\left(\frac{1}{(n+1)^s}-\frac{1}{(n+m+1)^s}\right)$$

und folglich auch kleiner als

$$\frac{C}{(n+1)^s}<\frac{C}{n^s};$$

die Summe dieser m Glieder der Reihe kann daher, wie gross ihre Anzahl m auch genommen werden mag, durch hinreichend grosse Werthe von n kleiner gemacht werden, als jeder vorher vorgeschriebene noch so kleine Werth. Das Stattfinden dieser Erscheinung ist aber bekanntlich nicht nur ein erforderliches, sondern auch ein ausreichendes Kennzeichen für die Convergenz einer jeden unendlichen Reihe.

Nachdem so für jeden positiven Werth von s die Convergenz der Reihe gezeigt ist, haben wir noch zu beweisen, dass der Werth der Reihe sich stetig mit s ändert; wir weisen dies nach für das Gebiet aller positiven Werthe von s, die grösser sind als ein bestimmter positiver Werth σ; da man nämlich, wie klein ein von Null verschiedener positiver Werth s auch sein mag, immer noch einen positiven Werth σ angeben kann, welcher unterhalb s liegt, so wird der Beweis dann wirklich für alle positiven Werthe s (excl. $s=0$) gelten. Nun können wir die ganze Reihe als aus zwei Theilen bestehend ansehen, deren erster die Summe ihrer ersten n Glieder

$$\beta_1\left(\frac{1}{1^s}-\frac{1}{2^s}\right)+\cdots+\beta_n\left(\frac{1}{n^s}-\frac{1}{(n+1)^s}\right),$$

also eine stetige Function von s ist, während der zweite, wie im Vorhergehenden bewiesen ist, sicher

$$<\frac{C}{n^s} \text{ und also auch } <\frac{C}{n^\sigma}$$

ist; dieser letztere Theil kann also durch die Wahl eines hinreichend grossen Werthes von n, d. h. durch eine zweckmässige Zerlegung der ganzen Reihe, kleiner gemacht werden, als irgend ein vorgeschriebener Werth; und zwar wird, was besonders wichtig ist, für alle Werthe von $s>\sigma$ dies durch einen und denselben

Werth von n, d. h. durch eine und dieselbe Zerlegung der unendlichen Reihe bewirkt werden. Da nun der erste Bestandtheil stetig ist, so kann eine etwaige Unstetigkeit des Ganzen nur von einer Unstetigkeit des zweiten Bestandtheils herrühren, und folglich muss, da dieser zweite Theil für alle in Betracht kommenden Werthe von s absolut genommen $< Cn^{-\sigma}$ ist, die Grösse einer plötzlichen Werthänderung beim Durchlaufen eines bestimmten Werthes von s jedenfalls $< 2Cn^{-\sigma}$ sein. Da wir aber durch zweckmässige Wahl von n diesen Werth beliebig klein machen können, so folgt, dass gar keine Unstetigkeit vorkommen kann; denn fände wirklich ein Sprung um eine Grösse μ Statt, so nehme man n so gross, dass $2Cn^{-\sigma} < \mu$ wird, so ergiebt sich augenblicklich der Widerspruch.

Nachdem so die Convergenz und Stetigkeit der zweiten und folglich auch die der ersten Reihe bewiesen ist, kehren wir zu unserer Reihe

$$\sum \delta^{\frac{1}{2}(n-1)}\, \varepsilon^{\frac{1}{8}(n^2-1)} \left(\frac{n}{P}\right) \frac{1}{n^s}$$

zurück, auf welche wir die eben entwickelten Principien anwenden wollen. Doch wird es zweckmässig sein, hier die vier verschiedenen Fälle von einander zu sondern, welche den verschiedenen Vorzeichen von δ und ε entsprechen.

§. 102.

Ist zunächst D ungerade und von der Form $4n+1$, so ist $\varepsilon = 1$ und $\delta = 1$, und wir haben daher die unendliche Reihe

$$\sum \left(\frac{n}{P}\right) \frac{1}{n^s}$$

zu betrachten, in welcher n alle positiven ungeraden Zahlen zu durchlaufen hat, die relative Primzahlen gegen P sind. Wir formen sie zunächst so um, dass die Summation auch auf die geraden Zahlen auszudehnen ist; dazu multipliciren wir sie mit der unendlichen Reihe

$$\frac{1}{1 - \left(\frac{2}{P}\right) \frac{1}{2^s}} = \sum \left(\frac{2^r}{P}\right) \frac{1}{(2^r)^s},$$

wo der Summationsbuchstabe r alle ganzen Zahlwerthe 0, 1, 2 3 . . . durchläuft; das Product dieser beiden unendlichen Reihen besteht, wenn man die Multiplication ausführt, aus Gliedern der Form

$$\left(\frac{2^r \cdot n}{P}\right) \frac{1}{(2^r \cdot n)^s} = \left(\frac{m}{P}\right) \frac{1}{m^s},$$

in welchen die Zahlen $m = 2^r \cdot n$ lauter (gerade und ungerade) relative Primzahlen gegen P sind; da umgekehrt jede relative Primzahl gegen P stets und nur auf eine einzige Weise in die Form $2^r \cdot n$ gebracht werden kann, so wird auf diese Weise jede solche relative Primzahl m einmal erzeugt, und es werden keine andern Zahlen erzeugt. Mithin ist das Product der beiden unendlichen Reihen gleich der unendlichen Reihe

$$\Sigma \left(\frac{m}{P}\right) \frac{1}{m^s}$$

und folglich ist

$$\Sigma \left(\frac{n}{P}\right) \frac{1}{n^s} = \left(1 - \left(\frac{2}{P}\right) \frac{1}{2^s}\right) \; \Sigma \left(\frac{m}{P}\right) \frac{1}{m^s}$$

wo also der Summationsbuchstabe m auf der rechten Seite alle positiven relativen Primzahlen gegen P zu durchlaufen hat; ja, man kann m alle ganzen positiven Zahlen ohne Ausnahme durchlaufen lassen, vorausgesetzt, dass (wie auch in den Supplementen I. §. 116 geschehen ist) dem Legendre'schen Symbol $\left(\frac{m}{P}\right)$ stets der Werth Null beigelegt wird, so oft m einen gemeinschaftlichen Divisor mit P hat. Die unendliche Reihe

$$\Sigma \left(\frac{m}{P}\right) \frac{1}{m^s}$$

hat nun für jeden Werth von $s > 1$ eine bestimmte von der Anordnung der Glieder unabhängige Summe; ordnen wir aber die Glieder so, dass m successive die Werthe 1, 2, 3 . . . durchläuft, so bildet diese Reihe einen speciellen Fall der oben betrachteten allgemeinen Reihe; denn es lässt sich leicht zeigen, dass die Summe der n ersten Coefficienten

$$\left(\frac{1}{P}\right) + \left(\frac{2}{P}\right) + \cdots + \left(\frac{n}{P}\right)$$

ihrem absoluten Werth nach stets unter einer endlichen Grenze bleibt, wie gross auch n genommen werden mag; aus den Supplementen (I. §. 116) oder auch aus §. 52 folgt nämlich, dass die Summe von je P aufeinander folgenden Symbolen, deren Zähler also ein vollständiges Restsystem nach dem Modul P bilden, $= 0$ ist, und hieraus ergiebt sich unmittelbar, dass die Summe von beliebig vielen aufeinander folgenden Symbolen absolut genommen stets unter $\frac{1}{2} P$ oder sogar unter $\frac{1}{2} \varphi(P)$ liegt. Mithin ist die so angeordnete unendliche Reihe eine convergirende und zugleich eine stetige Function von s, so lange s positiv ist; der Grenzwerth, welchem diese Reihe sich nähert, wenn s der Einheit unendlich nahe kommt, ist daher

$$\Sigma \left(\frac{m}{P}\right) \frac{1}{m},$$

und folglich wird

$$\lim \Sigma \left(\frac{D}{n}\right) \frac{1}{n^s} = \left(1 - \left(\frac{2}{P}\right) \frac{1}{2}\right) \; \Sigma \left(\frac{m}{P}\right) \frac{1}{m},$$

wo in der Summe rechts der Buchstabe m alle positiven Zahlen *der Reihe nach* durchlaufen muss.

§. 103.

Die nun noch auszuführende Summation kann mit Hülfe des in den Supplementen (I. §. 116) bewiesenen Satzes auf verschiedene Arten bewerkstelligt werden, entweder durch Zurückführung auf Fourier'sche Reihen, oder durch die Integration eines rationalen Bruchs. Wir schlagen den letztern Weg als den directern ein. Bedeutet m irgend eine positive Zahl, so ist bekanntlich

$$\frac{1}{m} = \int_0^1 x^{m-1} dx,$$

und folglich ist auch

$$\Sigma \left(\frac{m}{P}\right) \frac{1}{m} = \Sigma \left(\frac{m}{P}\right) \int_0^1 x^{m-1} dx.$$

Da nun der Coefficient $\left(\frac{m}{P}\right)$ für alle einander nach dem Modul

P congruenten Zahlen m denselben Werth hat, so ist die Summe der ersten kP Glieder unserer Reihe gleich

$$\int_0^1 \frac{1}{x} f(x) \frac{1 - x^{kP}}{1 - x^P} dx,$$

wo zur Abkürzung

$$f(x) = \Sigma \left(\frac{\mu}{P}\right) x^\mu$$

gesetzt ist, und der Summationsbuchstabe μ die P Werthe

$$1,\ 2,\ 3 \ldots P$$

durchlaufen muss. Da dieselben ein vollständiges Restsystem in Bezug auf den Modul P bilden, so ist nach einem schon öfter benutzten Satze

$$f(1) = \Sigma \left(\frac{\mu}{P}\right) = 0;$$

es ist folglich $f(x)$ theilbar durch $(x - 1)$, und mithin hat der Bruch

$$\frac{1}{x} \cdot \frac{f(x)}{1 - x^P} = F(x)$$

im ganzen Integrationsintervall endliche Werthe. Hieraus folgt leicht, dass mit unbegrenzt wachsendem k das Integral

$$\int_0^1 F(x) x^{kP} dx$$

unendlich klein wird, und wir erhalten folglich

$$\Sigma \left(\frac{m}{P}\right) \frac{1}{m} = \int_0^1 F(x)\, dx;$$

die Aufgabe ist mithin darauf zurückgeführt, einen echten rationalen Bruch zu integriren, was bekanntlich durch Zerlegung desselben in sogenannte Partialbrüche geschieht. Setzen wir zur Abkürzung

$$\sqrt{-1} = i,\ e^{\frac{2\pi i}{P}} = \theta,$$

so ist in unserm Fall der Nenner

$$x^P - 1 = \Pi\,(x - \theta^\alpha),$$

wo das Productzeichen sich auf den Buchstaben α bezieht, welcher ein vollständiges Restsystem in Bezug auf den Modul P durchlaufen muss; wir setzen fest, dass α die Werthe

$$0,\ 1,\ 2\ \ldots\ (P-1)$$

durchlaufen soll; man erhält dann nach bekannten Regeln

$$F(x) = -\frac{1}{P}\,\Sigma\,\frac{f(\theta^\alpha)}{x-\theta^\alpha},$$

wo das Summenzeichen sich auf den Buchstaben α bezieht. Nach der oben eingeführten Bezeichnung ist nun

$$f(\theta^\alpha) = \Sigma\left(\frac{\mu}{P}\right) e^{\mu\frac{2\alpha\pi i}{P}},$$

und diese Summe ist vermöge des in den Supplementen (I. §. 116) bewiesenen Satzes

$$= \left(\frac{\alpha}{P}\right) \sqrt{P}\cdot i^{1/4\,(P-1)^2}$$

wo die Quadratwurzel $\sqrt{P}$ positiv zu nehmen ist. Die Zerlegung in Partialbrüche liefert uns also das Resultat

$$F(x) = -\frac{i^{1/4\,(P-1)^2}}{\sqrt{P}}\,\Sigma\,\frac{\left(\frac{\alpha}{P}\right)}{x-\theta^\alpha},$$

wo das Summenzeichen sich auf den Buchstaben α bezieht, der nur alle die positiven ganzen Zahlen zu durchlaufen braucht, welche $< P$ und relative Primzahlen zu P sind; denn wenn α nicht relative Primzahl gegen P ist, so ist

$$\left(\frac{\alpha}{P}\right) = 0.$$

Die nun auszuführenden Integrationen der einzelnen $\varphi(P)$ Partialbrüche sind in der einen Formel

$$\int \frac{dx}{x-a-bi} = \tfrac{1}{2}\log\left\{(x-a)^2 + b^2\right\} + i\,\operatorname{arctang}\frac{x-a}{b}$$

oder

$$\int \frac{dx}{x - e^{\delta i}} = \tfrac{1}{2} \log \left\{ x^2 - 2x \cos\delta + 1 \right\} + i \operatorname{arctang} \frac{x - \cos\delta}{\sin\delta}$$

enthalten, aus welcher, wenn $0 < \delta < 2\pi$ ist,

$$\int_0^1 \frac{dx}{x - e^{\delta i}} =$$

$$\log(2 \sin \tfrac{1}{2}\delta) + i \left\{ \operatorname{arctang}(\operatorname{tang} \tfrac{1}{2}\delta) + \operatorname{arctang}(\operatorname{cotang}\delta) \right\}$$

folgt, vorausgesetzt, dass die beiden Arcus, welche in der Parenthese stehen, in dem Intervall zwischen $+\frac{1}{2}\pi$ und $-\frac{1}{2}\pi$ genommen werden. Mag nun δ zwischen 0 und π, oder zwischen π und 2π liegen, so ergiebt sich hieraus leicht, dass immer

$$\int_0^1 \frac{dx}{x - e^{\delta i}} = \log(2 \sin \tfrac{1}{2}\delta) + i\,(\tfrac{1}{2}\pi - \tfrac{1}{2}\delta)$$

ist.

Wenden wir dies auf unsern Fall an, so erhalten wir

$$\int_0^1 \frac{dx}{x - \theta^\alpha} = \log\left(2 \sin \frac{\alpha\pi}{P}\right) + i\left(\frac{\pi}{2} - \frac{\alpha\pi}{P}\right)$$

und folglich

$$\Sigma \left(\frac{m}{P}\right) \frac{1}{m} = - \frac{i^{1/4(P-1)^2}}{\sqrt{P}} \Sigma \left(\frac{\alpha}{P}\right) \left\{ \log\left(2 \sin \frac{\alpha\pi}{P}\right) + i\left(\frac{\pi}{2} - \frac{\alpha\pi}{P}\right) \right\},$$

wo das Summenzeichen rechts sich auf alle $\varphi(P)$ Werthe von α erstreckt. Da nun

$$\Sigma \left(\frac{\alpha}{P}\right) = 0$$

ist, so können die in der Parenthese befindlichen Glieder, welche von α unabhängig sind, wie $\log 2$ und $i\,\frac{1}{2}\pi$ weggelassen werden, und man erhält dann

$$\Sigma \left(\frac{m}{P}\right) \frac{1}{m} = - \frac{i^{1/4(P-1)^2}}{\sqrt{P}} \Sigma \left(\frac{\alpha}{P}\right) \left\{ \log \sin \frac{\alpha\pi}{P} - \frac{\alpha\pi i}{P} \right\}.$$

Dieses Resultat nimmt noch einfachere Formen an, wenn man die beiden Fälle $P \equiv 1 \pmod{4}$ und $P \equiv 3 \pmod{4}$ von einander trennt. Im erstern Falle ist nämlich

$$i^{1/4(P-1)^2} = 1$$

und folglich, da die linke Seite reell ist,

$$\Sigma \left(\frac{m}{P}\right) \frac{1}{m} = - \frac{1}{\sqrt{P}} \Sigma \left(\frac{\alpha}{P}\right) \log \sin \frac{\alpha \pi}{P}$$

$$\Sigma \left(\frac{\alpha}{P}\right) \alpha = 0;$$

im letztern Fall dagegen ist

$$i^{1/4(P-1)^2} = i$$

und folglich

$$\Sigma \left(\frac{m}{P}\right) \frac{1}{m} = - \frac{\pi}{P\sqrt{P}} \Sigma \left(\frac{\alpha}{P}\right) \alpha$$

$$\Sigma \left(\frac{\alpha}{P}\right) \log \sin \frac{\alpha \pi}{P} = 0.$$

Diese beiden Vereinfachungen lassen sich auch auf folgende Weise verificiren. Bedenkt man, dass $(P-\alpha)$ dieselben Werthe wie α durchläuft, so folgt

$$\Sigma \left(\frac{\alpha}{P}\right) \alpha = \Sigma \left(\frac{P-\alpha}{P}\right) (P-\alpha) = - \Sigma \left(\frac{-\alpha}{P}\right) \alpha$$

$$\Sigma \left(\frac{\alpha}{P}\right) \log \sin \frac{\alpha \pi}{P} = \Sigma \left(\frac{P-\alpha}{P}\right) \log \sin \frac{(P-\alpha)\pi}{P}$$

$$= \Sigma \left(\frac{-\alpha}{P}\right) \log \sin \frac{\alpha \pi}{P};$$

ist nun $P \equiv 1 \pmod{4}$, so folgt hieraus

$$\Sigma \left(\frac{\alpha}{P}\right) \alpha = - \Sigma \left(\frac{\alpha}{P}\right) \alpha = 0;$$

ist dagegen $P \equiv 3 \pmod{4}$, so ergiebt sich

$$\Sigma \left(\frac{\alpha}{P}\right) \log \sin \frac{\alpha \pi}{P} = - \Sigma \left(\frac{\alpha}{P}\right) \log \sin \frac{\alpha \pi}{P} = 0.$$

§. 104.

Hiermit ist nun für den von uns betrachteten Fall, in welchem die Determinante $D = \pm P \equiv 1 \pmod{4}$ und durch kein Quadrat theilbar ist, der gesuchte Grenzwerth

$$\lim \Sigma \left(\frac{D}{n}\right) \frac{1}{n^s} = \left(1 - \left(\frac{2}{P}\right) \frac{1}{2}\right) \Sigma \left(\frac{m}{P}\right) \frac{1}{m}$$

wirklich in Form eines geschlossenen Ausdrucks gefunden, und um die Anzahl h der zu dieser Determinante D gehörenden ursprünglichen Formen der ersten Art zu erhalten, brauchen wir nur noch die beiden Fälle, in welchen D negativ oder positiv ist, von einander zu trennen.

Erstens. Ist D negativ $= - P$, und also $P \equiv 3 \pmod{4}$, so ist (§. 97)

$$h = \frac{2\sqrt{-D}}{\pi} \lim \Sigma \left(\frac{D}{n}\right) \frac{1}{n^s}$$

und da in diesem Fall

$$\lim \Sigma \left(\frac{D}{n}\right) \frac{1}{n^s} = \left(1 - \left(\frac{2}{P}\right) \frac{1}{2}\right) \Sigma \left(\frac{m}{P}\right) \frac{1}{m}$$
$$= - \left(1 - \left(\frac{2}{P}\right) \frac{1}{2}\right) \frac{\pi}{P\sqrt{P}} \Sigma \left(\frac{\alpha}{P}\right) \alpha$$

ist, so ergiebt sich

$$h = - \frac{1}{P} \left(2 - \left(\frac{2}{P}\right)\right) \Sigma \left(\frac{\alpha}{P}\right) \alpha,$$

wo α wieder alle positiven ganzen Zahlen durchlaufen muss, die $< P$ und relative Primzahlen zu P sind. Offenbar muss dieser Ausdruck für die Classenanzahl sich noch in der Weise umformen lassen, dass der Divisor P verschwindet. Dies lässt sich in der That durch folgende Betrachtung erreichen. Bezeichnet man mit α' diejenigen Zahlen α, welche $< \frac{1}{2} P$ sind, so stimmen die Zahlen $(P - \alpha')$ mit denjenigen Zahlen α überein, welche $> \frac{1}{2} P$ sind; es ist daher

$$\Sigma \left(\frac{\alpha}{P}\right) \alpha = \Sigma \left(\frac{\alpha'}{P}\right) \alpha' + \Sigma \left(\frac{P - \alpha'}{P}\right) (P - \alpha'),$$

wo die Summenzeichen rechts sich auf den Buchstaben α' beziehen; da nun $P \equiv 3 \pmod{4}$ und also

$$\left(\frac{P-\alpha'}{P}\right) = \left(\frac{-1}{P}\right)\left(\frac{\alpha'}{P}\right) = -\left(\frac{\alpha'}{P}\right)$$

ist, so erhalten wir

$$\Sigma\left(\frac{\alpha}{P}\right)\alpha = 2\,\Sigma\left(\frac{\alpha'}{P}\right)\alpha' - P\,\Sigma\left(\frac{\alpha'}{P}\right).$$

Offenbar wird die Reihe aller Zahlen α aber auch erschöpft durch die sämmtlichen Zahlen $2\alpha'$ und $(P-2\alpha')$, und folglich ist auch

$$\Sigma\left(\frac{\alpha}{P}\right)\alpha = \Sigma\left(\frac{2\alpha'}{P}\right)2\alpha' + \Sigma\left(\frac{P-2\alpha'}{P}\right)(P-2\alpha')$$

oder nach leichten Reductionen

$$\left(\frac{2}{P}\right)\Sigma\left(\frac{\alpha}{P}\right)\alpha = 4\,\Sigma\left(\frac{\alpha'}{P}\right)\alpha' - P\,\Sigma\left(\frac{\alpha'}{P}\right).$$

Zieht man diese Gleichung von der frühern ab, nachdem dieselbe mit 2 multiplicirt ist, so erhält man

$$\left\{2 - \left(\frac{2}{P}\right)\right\}\Sigma\left(\frac{\alpha}{P}\right)\alpha = -P\,\Sigma\left(\frac{\alpha'}{P}\right)$$

und hierdurch verwandelt sich der obige Ausdruck für die Classenanzahl in den folgenden einfachsten:

$$h = \Sigma\left(\frac{\alpha'}{P}\right).$$

Wir können daher für diesen Fall als Resultat unserer ganzen Untersuchung folgenden Satz aussprechen:

Ist P eine positive, durch kein Quadrat theilbare Zahl von der Form $4n+3$, und bezeichnet man mit α' alle relativen Primzahlen zu P, welche $< \frac{1}{2}P$ sind, so findet man die Classenanzahl h der zu der Determinante $D = -P$ gehörenden Formen der ersten Art, wenn man von der Anzahl derjenigen der Zahlen α', für welche

$$\left(\frac{\alpha'}{P}\right) = +1$$

ist, die Anzahl der übrigen Zahlen α' abzieht.

Der Ausdruck dieses Satzes vereinfacht sich in dem speciellen Fall, wenn P eine einfache Primzahl ist, folgendermaassen

Ist der absolute Werth p der negativen Determinante $D = -p$ eine Primzahl von der Form $4n + 3$, so ist die Classenanzahl h der zu ihr gehörigen Formen der ersten Art gleich dem Ueberschuss der Anzahl der zwischen 0 und $\frac{1}{2}p$ liegenden quadratischen Reste von p über die Anzahl der zwischen denselben Grenzen liegenden quadratischen Nichtreste von p.

Dieser letztere Satz ist in einer nicht wesentlich verschiedenen Form schon einige Zeit vor der Veröffentlichung der Lösung des allgemeinen Problems *) durch Induction von *Jacobi* **) gefunden.

Als Beispiel wählen wir die Determinante $D = -11$; unter den Zahlen 1, 2, 3, 4, 5 sind vier quadratische Reste 1, 3, 4, 5, und ein quadratischer Nichtrest 2 von 11; mithin ist die Anzahl der Formen erster Art $= 4 - 1 = 3$. In der That giebt es für diese Determinante nur drei (nicht äquivalente) reducirte Formen erster Art, nämlich (1, 0, 11), (3, 1, 4) und (3, − 1, 4).

Beiläufig mag hier bemerkt werden, dass zufolge des gewonnenen Resultats die Anzahl der Zahlen α', für welche

$$\left(\frac{\alpha'}{P}\right) = +1$$

stets grösser ist, als die Anzahl der Zahlen α', für welche

$$\left(\frac{\alpha'}{P}\right) = -1$$

ist, da h immer eine positive Zahl, nie $= 0$ ist: ein Satz, welcher auch für den einfachsten Fall, wo P eine Primzahl von der Form $4n + 3$ ist, auf anderm Wege noch nicht hat bewiesen werden können (vergl. das Theorem über die arithmetische Progression, Supplemente VI. §. 137).

Zweitens. Ist die Determinante D positiv $= + P$, und also $P \equiv 1 \pmod{4}$, so ist (nach §. 99) die Classenanzahl

$$h = \frac{2\sqrt{D}}{\log(T + U\sqrt{D})} \lim \Sigma \left(\frac{D}{n}\right) \frac{1}{n^s}$$

---

*) *Dirichlet*: *Recherches sur diverses applications de l'analyse infinitésimale à la théorie des nombres* in Crelle's Journal XIX und XXI.

**) *Observatio arithmetica* in Crelle's Journal IX; vergl. *Dirichlet*: *Gedächtnissrede auf C. G. J. Jacobi* und *Kummer*: *Gedächtnissrede auf G. P. Lejeune-Dirichlet.*

und da in diesem Fall

$$\lim \Sigma \left(\frac{D}{n}\right)\frac{1}{n^s} = \left(1 - \left(\frac{2}{P}\right)\frac{1}{2}\right)\Sigma\left(\frac{m}{P}\right)\frac{1}{m}$$

$$= -\frac{1 - \left(\frac{2}{P}\right)\frac{1}{2}}{\sqrt{P}}\Sigma\left(\frac{\alpha}{P}\right)\log\sin\frac{\alpha\pi}{P}$$

ist, so ergiebt sich

$$h = -\frac{2 - \left(\frac{2}{P}\right)}{\log(T + U\sqrt{P})}\Sigma\left(\frac{\alpha}{P}\right)\log\sin\frac{\alpha\pi}{P}.$$

Bezeichnet man die Zahlen α mit a oder mit b, je nachdem

$$\left(\frac{\alpha}{P}\right) = +1 \text{ oder } = -1$$

ist, so nimmt die vorstehende Gleichung folgende Gestalt an:

$$h = \frac{2 - \left(\frac{2}{P}\right)}{\log(T + U\sqrt{P})}\log\frac{\Pi\sin\frac{b\pi}{P}}{\Pi\sin\frac{a\pi}{P}};$$

hierin beziehen sich die Productzeichen Π im Zähler und Nenner resp. auf alle b und auf alle a; und ausserdem bedeuten T, U die kleinsten positiven ganzen Zahlen, welche der Pell'schen Gleichung

$$T^2 - PU^2 = 1$$

genügen. Der wahre Charakter dieses Resultates wird durch eine weitere Umformung (§. 107) noch deutlicher werden.

§. 105.

Nachdem in den vorhergehenden §§. 102 — 104 der Fall, in welchem $D \equiv 1 \pmod{4}$ ist, seine vollständige Behandlung gefunden hat, begnügen wir uns, bei der Betrachtung der übrigen Fälle, die Hauptmomente hervorzuheben. Es handelt sich hauptsächlich um die Bestimmung des Grenzwerthes der Reihe

$$\Sigma \left(\frac{D}{n}\right) \frac{1}{n^s} = \Sigma\, \delta^{1/2(n-1)}\, \varepsilon^{1/8(n^2-1)} \left(\frac{n}{P}\right) \frac{1}{n^s},$$

in welcher der Buchstabe n alle positiven ganzen Zahlen durchlaufen muss, die relative Primzahlen zu $2\,P$ sind.

1) Wir bezeichnen mit ν diejenigen Zahlen n, welche $< 8\,P$ sind, und deren Anzahl $= \varphi(8\,P) = 4\,\varphi(P)$ ist; wir setzen ferner zur Abkürzung

$$f(x) = \Sigma\, \delta^{1/2(\nu-1)}\, \varepsilon^{1/8(\nu^2-1)} \left(\frac{\nu}{P}\right) x^\nu,$$

wo das Summenzeichen sich auf alle Werthe ν erstreckt, und stellen uns die Aufgabe, den Werth $f(\omega)$ zu bestimmen, welchen die ganze rationale Function $f(x)$ für $x = \omega$ annimmt, wo

$$\omega = e^{\frac{2 m \pi i}{8 P}}$$

irgend eine Wurzel der Gleichung

$$\omega^{8P} = 1$$

bedeutet.

Für jeden bestimmten Werth ν haben die beiden Congruenzen

$$8\,\alpha \equiv \nu \text{ (mod. } P), \quad P\gamma \equiv \nu \text{ (mod. 8)}$$

vollständig bestimmte Wurzeln α (mod. P) und γ (mod. 8), und da gleichzeitig

$$\nu \equiv 8\alpha + P\gamma \text{ (mod. } P), \text{ und } \nu \equiv 8\alpha + P\gamma \text{ (mod. 8)},$$

so ist auch

$$\nu \equiv 8\alpha + P\gamma \text{ (mod. } 8P);$$

durchläuft α ein vollständiges System von $\varphi(P)$ Zahlen, die relative Primzahlen zu P und unter einander (mod. P) incongruent sind, und durchläuft γ die Zahlen 1, 3, 5, 7, so wird der Ausdruck $8\,\alpha + P\gamma$ jeder der Zahlen ν einmal und auch nur einmal nach dem Modul $8\,P$ congruent werden (vergl. §. 25). Dann ist

$$\delta^{1/2(\nu-1)} = \delta^{1/2(P\gamma-1)} = \delta^{1/2(P-1)}\, \delta^{1/2(\gamma-1)}$$

$$\varepsilon^{1/8(\nu^2-1)} = \varepsilon^{1/8(P^2\gamma^2-1)} = \varepsilon^{1/8(P^2-1)}\, \varepsilon^{1/8(\gamma^2-1)}$$

$$\left(\frac{\nu}{P}\right) = \left(\frac{8\,\alpha}{P}\right) = \left(\frac{2}{P}\right)\left(\frac{\alpha}{P}\right)$$

$$\omega^\nu = \omega^{8\alpha+P\gamma} = e^{\alpha\frac{2m\pi i}{P}} . e^{\gamma\frac{2m\pi i}{8}} = \theta^{\alpha m}\, j^{\gamma m},$$

wenn man zur Abkürzung

$$\theta = e^{\frac{2\pi i}{P}},\; j = e^{\frac{\pi i}{4}} = \frac{1+i}{\sqrt{2}}$$

setzt, und folglich

$$f(\omega) = \delta^{\frac{1}{2}(P-1)}\, \varepsilon^{\frac{1}{8}(P^2-1)} \left(\frac{2}{P}\right) \cdot \sum \delta^{\frac{1}{2}(\gamma-1)}\, \varepsilon^{\frac{1}{8}(\gamma^2-1)}\, j^{\gamma m} \cdot \sum \left(\frac{\alpha}{P}\right) \theta^{\alpha m},$$

wo das erste Summenzeichen sich auf die vier Werthe von γ, das zweite sich auf die $\varphi(P)$ Werthe von α bezieht. Für die erste dieser beiden Summen findet man leicht den Werth

$$j^m(1 + \delta i^{3m})\,(1 + \varepsilon(-1)^m);$$

ferner ist die zweite dieser beiden Summen (Supplemente I. §. 116) gleich

$$\left(\frac{m}{P}\right) i^{\left(\frac{P-1}{2}\right)^2} \sqrt{P},$$

wo die Quadratwurzel, wie immer im Folgenden, positiv zu nehmen ist. Hieraus folgt

$$f(\omega) = f\left(e^{\frac{2m\pi i}{8P}}\right) = K\psi(m),$$

wenn zur Abkürzung

$$K = \delta^{\frac{1}{2}(P-1)}\, \varepsilon^{\frac{1}{8}(P^2-1)}\, i^{\left(\frac{P-1}{2}\right)^2} \left(\frac{2}{P}\right) \sqrt{P},$$

$$\psi(m) = j^m(1 + \delta i^{3m})\,(1 + \varepsilon(-1)^m) \left(\frac{m}{P}\right)$$

gesetzt wird.

Aus dem so erhaltenen Ausdruck, oder noch einfacher aus der unmittelbaren Definition

$$f(\omega) = \sum \delta^{\frac{1}{2}(\nu-1)}\, \varepsilon^{\frac{1}{8}(\nu^2-1)} \left(\frac{\nu}{P}\right) \omega^\nu$$

folgt leicht, dass die Summe aller, den $8P$ verschiedenen Wurzeln ω entsprechenden, Werthe von $f(\omega)$ gleich Null ist; denn da ν relative Primzahl zu $8P$ ist, so ist

$$\Sigma' \omega^\nu = 1 + e^{\frac{2\nu\pi i}{8P}} + e^{\frac{4\nu\pi i}{8P}} + \cdots + e^{\frac{2(8P-1)\nu\pi i}{8P}} = 0,$$

und folglich auch

$$\Sigma' f(\omega) = \Sigma\, \delta^{\frac{1}{2}(\nu-1)} \,.\, \varepsilon^{\frac{1}{8}(\nu^2-1)} \left(\frac{\nu}{P}\right) \Sigma' \,\omega^\nu = 0,$$

wo das Summenzeichen Σ' sich auf die $8P$ verschiedenen Werthe von ω bezieht.

2) Setzen wir in dem für $f(\omega)$ gefundenen Ausdruck $\omega = 1$, also $m \equiv 0 \pmod{8P}$, so wird, wenn P nicht $= 1$ ist, $\left(\frac{m}{P}\right)$ und folglich auch $f(\omega) = 0$; ist aber $P = 1$ und folglich (da D nicht $= 1$ ist) mindestens eine der beiden Einheiten δ oder $\varepsilon = -1$, so ist auch mindestens einer der beiden Factoren

$$1 + \delta i^{3m} = 1 + \delta, \;\; 1 + \varepsilon(-1)^m = 1 + \varepsilon$$

gleich Null, und folglich ist in jedem Fall

$$f(1) = \Sigma\, \delta^{\frac{1}{2}(\nu-1)}\, \varepsilon^{\frac{1}{8}(\nu^2-1)} \left(\frac{\nu}{P}\right) = 0.$$

Ordnet man nun die Glieder der unendlichen Reihe

$$\Sigma \left(\frac{D}{n}\right) \frac{1}{n^s} = \Sigma\, \delta^{\frac{1}{2}(n-1)}\, \varepsilon^{\frac{1}{8}(n^2-1)} \left(\frac{n}{P}\right) \frac{1}{n^s}$$

so, dass sie Zahlen n wachsen, so folgt hieraus, dass die Summe der Coefficienten von je $\varphi(8P)$ aufeinander folgenden Gliedern $= 0$ ist, und dass also die Summe von beliebig vielen solchen auf einander folgenden Coefficienten ihrem absoluten Werth nach den endlichen Werth $\frac{1}{2}\varphi(8P) = 2\varphi(P)$ nie übersteigt. Mithin ist die so angeordnete Reihe (nach §. 101) eine für alle positiven Werthe von s endliche und stetige Function von s; der zu bestimmende Grenzwerth ist daher

$$\Sigma \left(\frac{D}{n}\right) \frac{1}{n} = \Sigma\, \delta^{\frac{1}{2}(n-1)}\, \varepsilon^{\frac{1}{8}(n^2-1)} \left(\frac{n}{P}\right) \frac{1}{n},$$

wo die Zahlen n ihrer Grösse nach aufeinander folgen müssen, und man findet durch Anwendung der Formel

$$\frac{1}{n} = \int_0^1 x^{n-1}\, dx,$$

ähnlich wie in §. 103,

$$\Sigma\left(\frac{D}{n}\right)\frac{1}{n} = \int_0^1 \frac{1}{x}\cdot\frac{f(x)\,dx}{1-x^{8P}}.$$

Bezeichnet man wieder mit

$$\omega = e^{\frac{2m\pi i}{8P}}$$

die sämmtlichen Wurzeln der Gleichung $\omega^{8P} = 1$, so ist

$$\frac{1}{x}\cdot\frac{f(x)}{1-x^{8P}} = -\frac{1}{8P}\Sigma\frac{f(\omega)}{x-\omega};$$

da $f(1) = 0$ ist, so fällt der von der Wurzel $\omega = 1$, d. h. der von der Zahl $m \equiv 0 \pmod{8P}$ herrührende Bestandtheil weg; wählen wir ferner die übrigen Zahlen m so, dass sie zwischen 0 und $8P$ liegen, so ist (nach §. 103)

$$\int_0^1 \frac{dx}{x-\omega} = \log\left(2\sin\frac{m\pi}{8P}\right) + i\left(\frac{\pi}{2}-\frac{m\pi}{8P}\right)$$

und folglich

$$\Sigma\left(\frac{D}{n}\right)\frac{1}{n} = -\frac{K}{8P}\Sigma\,\psi(m)\left\{\log\left(2\sin\frac{m\pi}{8P}\right) + i\left(\frac{\pi}{2}-\frac{m\pi}{8P}\right)\right\},$$

wo rechts alle Glieder fortgelassen werden können, für welche $\psi(m) = 0$ ist; da ferner, wie oben gezeigt ist,

$$\Sigma f(\omega) = K\,\Sigma\,\psi(m) = 0$$

ist, so erhält man einfacher

$$\Sigma\left(\frac{D}{n}\right)\frac{1}{n} = -\frac{K}{8P}\Sigma\,\psi(m)\left\{\log\sin\frac{m\pi}{8P} - i\,\frac{m\pi}{8P}\right\}.$$

Wir trennen nun wieder die verschiedenen Fälle von einander.

3) Ist $D = \pm P \equiv 1 \pmod 4$, also $\delta = \varepsilon = +1$, so ist

$$\psi(m) = 4j^m\left(\frac{m}{P}\right) \text{ oder } = 0,$$

je nachdem m durch 4 theilbar ist oder nicht, und

$$K = i^{\left(\frac{P-1}{2}\right)^2}\left(\frac{2}{P}\right)\sqrt{P}.$$

Bezeichnet man daher mit μ alle zwischen 0 und $2P$ liegenden Zahlen, so kann man $m = 4\mu$ setzen und erhält

$$\Sigma \left(\frac{D}{n}\right) \frac{1}{n} = - \frac{i^{\left(\frac{P-1}{2}\right)^2}}{2\sqrt{P}} \left(\frac{2}{P}\right) \Sigma\, (-1)^\mu \left(\frac{\mu}{P}\right) \left\{\log \sin \frac{\mu\pi}{2P} - i \frac{\mu\pi}{2P}\right\};$$

nach einigen nicht schwierigen Umformungen findet man schliesslich dasselbe Resultat, wie früher (in §§. 103 und 104), nämlich für eine negative Determinante $D = -P$:

$$\Sigma \left(\frac{D}{n}\right) \frac{1}{n} = \frac{\pi}{2\sqrt{P}} \Sigma \left(\frac{\alpha}{P}\right),$$

wo der Buchstabe α alle relativen Primzahlen zu P durchlaufen muss, die $< \frac{1}{2} P$ sind; und für eine positive Determinante $D = +P$:

$$\Sigma \left(\frac{D}{n}\right) \frac{1}{n} = - \frac{2 - \left(\frac{2}{P}\right)}{2\sqrt{P}} \Sigma \left(\frac{m}{P}\right) \log \sin \frac{m}{P},$$

wo der Buchstabe m alle relativen Primzahlen zu P durchlaufen muss, die $< P$ sind.

4) Ist $D = \pm P \equiv 3 \pmod{4}$, also $\delta = -1$, $\varepsilon = +1$, so ist

$$\psi(m) = 4 j^m \left(\frac{m}{P}\right) \text{ oder } = 0,$$

je nachdem $m \equiv 2 \pmod{4}$ ist oder nicht, und

$$K = (-1)^{\frac{1}{2}(P-1)}\, i^{\left(\frac{P-1}{2}\right)^2} \left(\frac{2}{P}\right) \sqrt{P};$$

man kann daher m durch $2m$ ersetzen und erhält

$$\Sigma \left(\frac{D}{n}\right) \frac{1}{n} = - \frac{i^{\left(\frac{P+1}{2}\right)^2}}{2\sqrt{P}} \Sigma \left(\frac{-1}{m}\right) \left(\frac{m}{P}\right) \left\{\log \sin \frac{m\pi}{4P} - i \frac{m\pi}{4P}\right\},$$

wo m alle ungeraden Zahlen zwischen 0 und $4P$ durchlaufen muss; trennt man die positiven Determinanten von den negativen, so ergiebt sich für $D = +P$:

$$\Sigma \left(\frac{D}{n}\right) \frac{1}{n} = - \frac{1}{2\sqrt{P}} \Sigma \left(\frac{-1}{m}\right) \left(\frac{m}{P}\right) \log \sin \frac{m\pi}{4P},$$

und für $D = - P$:

$$\Sigma \left(\frac{D}{n}\right) \frac{1}{n} = - \frac{\pi}{8 P \sqrt{P}} \Sigma \left(\frac{-1}{m}\right) \left(\frac{m}{P}\right) m.$$

Der zweite dieser beiden Ausdrücke, welcher dem Fall $P \equiv 1 \pmod{4}$ entspricht, giebt für $P = 1$ (also $D = -1$) das bekannte Resultat

$$\Sigma\, (-1)^{\frac{1}{2}(n-1)} \frac{1}{n} = \frac{\pi}{4};$$

ist aber $P > 1$, so lässt er sich folgendermaassen vereinfachen. Bezeichnet man wieder mit α' alle Zahlen zwischen 0 und $\frac{1}{2} P$, so zerfallen die Zahlen m in die Zahlen

$$P - 2\alpha',\ P + 2\alpha',\ 3P - 2\alpha',\ 3P + 2\alpha',$$

und hieraus ergiebt sich leicht

$$\Sigma \left(\frac{-1}{m}\right) \left(\frac{m}{P}\right) m = - 4 P \left(\frac{2}{P}\right) \Sigma\, (-1)^{\alpha'} \left(\frac{\alpha'}{P}\right);$$

da ferner

$$\left(\frac{P - \alpha'}{P}\right) = \left(\frac{\alpha'}{P}\right)$$

und folglich

$$\Sigma \left(\frac{\alpha'}{P}\right) = 0$$

ist, so erhält man

$$\Sigma\, (-1)^{\alpha'} \left(\frac{\alpha'}{P}\right) = \Sigma \left\{1 + (-1)^{\alpha'}\right\} \left(\frac{\alpha'}{P}\right) = 2\, \Sigma \left(\frac{2\alpha}{P}\right),$$

wo mit α alle Zahlen zwischen 0 und $\frac{1}{4} P$ bezeichnet sind, und folglich

$$\Sigma \left(\frac{-1}{m}\right) \left(\frac{m}{P}\right) m = - 8 P\, \Sigma \left(\frac{\alpha}{P}\right)$$

$$\Sigma \left(\frac{D}{n}\right) \frac{1}{n} = \frac{\pi}{\sqrt{P}}\, \Sigma \left(\frac{\alpha}{P}\right).$$

5) Ist $D = \pm 2 P \equiv 2 \pmod{8}$, also $\delta = +1$, $\varepsilon = -1$, so ist

$$\psi(m) = 0 \quad \text{oder} \quad = 2\left(\frac{2}{m}\right)\left(\frac{m}{P}\right)\sqrt{2},$$

je nachdem m gerade oder ungerade, und

$$K = i^{\left(\frac{P-1}{2}\right)^2}\sqrt{P},$$

folglich

$$\Sigma\left(\frac{D}{n}\right)\frac{1}{n} = -\frac{i^{\left(\frac{P-1}{2}\right)^2}}{2\sqrt{2P}}\,\Sigma\left(\frac{2}{m}\right)\left(\frac{m}{P}\right)\left\{\log\sin\frac{m\pi}{8P} - i\,\frac{m\pi}{8P}\right\},$$

wo der Buchstabe m alle ungeraden Zahlen zwischen 0 und $8P$ zu durchlaufen hat. Trennt man die positiven Determinanten von den negativen, so erhält man für $D = +2P$:

$$\Sigma\left(\frac{D}{n}\right)\frac{1}{n} = -\frac{1}{2\sqrt{2P}}\,\Sigma\left(\frac{2}{m}\right)\left(\frac{m}{P}\right)\log\sin\frac{m\pi}{8P},$$

und für $D = -2P$:

$$\Sigma\left(\frac{D}{n}\right)\frac{1}{n} = -\frac{\pi}{16P\sqrt{2P}}\,\Sigma\left(\frac{2}{m}\right)\left(\frac{m}{P}\right)m.$$

Der zweite dieser beiden Ausdrücke, welcher dem Fall $P \equiv 3$ (mod. 4) entspricht, lässt sich bedeutend vereinfachen. Bezeichnet man mit γ diejenige der vier Zahlen $+1$, -1, $+3$, -3, welche der Congruenz

$$P\gamma \equiv m \pmod{8}$$

genügt, so kann man

$$m = P\gamma + 8\alpha$$

setzen; giebt man γ jeden der obigen vier Werthe und entsprechend dem Buchstaben α alle P Werthe, welche zwischen $-\frac{1}{8}P\gamma$ und $P - \frac{1}{8}P\gamma$ liegen, so nimmt der Ausdruck $P\gamma + 8\alpha$ jeden der $4P$ Werthe m einmal und auch nur einmal an; dann ist gleichzeitig

$$\left(\frac{2}{m}\right)\left(\frac{m}{P}\right) = \left(\frac{2}{\gamma}\right)\left(\frac{\alpha}{P}\right)$$

und hieraus folgt

$$\Sigma\left(\frac{2}{m}\right)\left(\frac{m}{P}\right)m = \Sigma\left(\frac{2}{\gamma}\right)\Sigma\left(\frac{\alpha}{P}\right)(P\gamma + 8\alpha),$$

wo die Summation in Bezug auf α zwischen den von γ abhängigen Grenzen auszuführen ist. Da nun $\sum\left(\frac{\alpha}{P}\right) = 0$ ist, wenn α irgend ein vollständiges Restsystem (mod. P) durchläuft, so kann man einfacher schreiben

$$\sum\left(\frac{2}{m}\right)\left(\frac{m}{P}\right) m = 8\sum\left(\frac{2}{\gamma}\right)\sum\left(\frac{\alpha}{P}\right)\alpha.$$

Beachtet man nun, wie oft ein und dasselbe α in den vier, den verschiedenen Werthen von γ entsprechenden, Summen vorkommt, so wird man bald finden, dass

$$\sum\left(\frac{2}{m}\right)\left(\frac{m}{P}\right) m = -16P\sum\left(\frac{\alpha}{P}\right)$$

und also

$$\sum\left(\frac{D}{n}\right)\frac{1}{n} = \frac{\pi}{\sqrt{2P}}\sum\left(\frac{\alpha}{P}\right)$$

ist, wo der Buchstabe α alle zwischen $\frac{1}{8}P$ und $\frac{3}{8}P$ liegenden Werthe durchlaufen muss.

6) Ist $D = \pm 2P \equiv 6$ (mod. 8), also $\delta = -1$, $\varepsilon = -1$, so ist

$$\psi(m) = 0 \text{ oder } = 2i\left(\frac{-2}{m}\right)\left(\frac{m}{P}\right)\sqrt{2}$$

je nachdem m gerade oder ungerade, und

$$K = (-1)^{\frac{1}{2}(P-1)}\, i^{\left(\frac{P-1}{2}\right)^2}\sqrt{P},$$

folglich

$$\sum\left(\frac{D}{n}\right)\frac{1}{n} = -\frac{i^{\left(\frac{P+1}{2}\right)^2}}{2\sqrt{2P}}\sum\left(\frac{-2}{m}\right)\left(\frac{m}{P}\right)\left\{\log\sin\frac{m\pi}{8P} - i\,\frac{m\pi}{8P}\right\},$$

wo der Buchstabe m alle ungeraden Zahlen zwischen 0 und $8P$ zu durchlaufen hat. Sondert man die Fälle von einander, in denen die Determinante positiv oder negativ ist, so erhält man für $D = +2P$:

$$\sum\left(\frac{D}{n}\right)\frac{1}{n} = -\frac{1}{2\sqrt{2P}}\sum\left(\frac{-2}{m}\right)\left(\frac{m}{P}\right)\log\sin\frac{m\pi}{8P},$$

und für $D = -2P$:

$$\Sigma\left(\frac{D}{n}\right)\frac{1}{n} = -\frac{\pi}{16P\sqrt{2P}}\Sigma\left(\frac{-2}{m}\right)\left(\frac{m}{P}\right)m.$$

Der letztere dieser beiden Ausdrücke, welcher dem Fall $P \equiv 1$ (mod. 4) entspricht, lässt sich wieder vereinfachen, wenn man

$$m = 8\alpha + P\gamma$$

setzt. Es wird dann

$$\left(\frac{-2}{m}\right)\left(\frac{m}{P}\right) = \left(\frac{-2}{\gamma}\right)\left(\frac{\alpha}{P}\right)$$

und folglich

$$\Sigma\left(\frac{-2}{m}\right)\left(\frac{m}{P}\right)m = 8\,\Sigma\left(\frac{-2}{\gamma}\right)\Sigma\left(\frac{\alpha}{P}\right)\alpha,$$

wo das von α zu durchlaufende Restsystem (mod. P) von dem Werth γ abhängt; untersucht man wieder, wie oft ein und derselbe Rest α in den vier, den verschiedenen Werthen γ entsprechenden, Summen vorkommt, so findet man ohne Schwierigkeit

$$\Sigma\left(\frac{-2}{m}\right)\left(\frac{m}{P}\right)m = -16P\left\{\Sigma\left(\frac{\alpha}{P}\right) - \Sigma\left(\frac{\alpha'}{P}\right)\right\}$$

und hieraus

$$\Sigma\left(\frac{D}{n}\right)\frac{1}{n} = \frac{\pi}{\sqrt{2P}}\left\{\Sigma\left(\frac{\alpha}{P}\right) - \Sigma\left(\frac{\alpha'}{P}\right)\right\},$$

wo α alle zwischen 0 und $\frac{1}{8}P$, und α' alle zwischen $\frac{3}{8}P$ und $\frac{1}{2}P$ liegenden Werthe durchlaufen muss.

Bei dieser Umformung war stillschweigend angenommen, dass $P > 1$; für den Fall $P = 1$ erhält man unmittelbar

$$\Sigma\left(\frac{-2}{m}\right)\left(\frac{m}{P}\right)m = 1 + 3 - 5 - 7 = -8$$

und folglich

$$\Sigma\left(\frac{D}{n}\right)\frac{1}{n} = \Sigma\left(\frac{-2}{n}\right)\frac{1}{n} = \frac{\pi}{2\sqrt{2}}.$$

§. 106.

Nachdem im vorhergehenden §. der Grenzwerth der unendlichen Reihe

$$\Sigma\left(\frac{D}{n}\right)\frac{1}{n^s}$$

für alle Fälle bestimmt ist, in welchen die Determinante D durch kein Quadrat (ausser 1) theilbar ist, können wir nun die Anzahl h der Classen der ursprünglichen Formen der ersten Art in geschlossener Form angeben *).

A. Für *negative* Determinanten ist (nach §. 97)

$$h = \frac{2\sqrt{-D}}{\pi}\cdot\Sigma\left(\frac{D}{n}\right)\frac{1}{n},$$

mit Ausnahme des Falles $D = -1$, wo der Ausdruck rechter Hand zu verdoppeln ist. Hieraus ergeben sich folgende vier Fälle:

I. $D = -P$; $P \equiv 3 \pmod{4}$;

$$h = \Sigma\left(\frac{\alpha}{P}\right);\ 0 < \alpha < \tfrac{1}{2}P.$$

II. $D = -P$; $P \equiv 1 \pmod{4}$;

$$h = 2\,\Sigma\left(\frac{\alpha}{P}\right);\ 0 < \alpha < \tfrac{1}{4}P;$$

hiervon ist auszunehmen der Fall

$$D = -1;\ h = 1.$$

III. $D = -2P$; $P \equiv 3 \pmod{4}$;

$$h = 2\,\Sigma\left(\frac{\alpha}{P}\right);\ \tfrac{1}{8}P < \alpha < \tfrac{3}{8}P.$$

IV. $D = -2P$; $P \equiv 1 \pmod{4}$;

$$h = 2\left\{\Sigma\left(\frac{\alpha}{P}\right) - \Sigma\left(\frac{\alpha'}{P}\right)\right\};\ \begin{array}{c} 0 < \alpha < \tfrac{1}{8}P; \\ \tfrac{3}{8}P < \alpha' < \tfrac{1}{2}P; \end{array}$$

hiervon ist auszunehmen der Fall

$$D = -2;\ h = 1.$$

B. Für *positive* Determinanten ist (nach §. 99)

$$h = \frac{2\sqrt{D}}{\log(T + U\sqrt{D})}\cdot\Sigma\left(\frac{D}{n}\right)\frac{1}{n},$$

*) In neuester Zeit hat *Kronecker* aus der Theorie der elliptischen Functionen neue Formeln zur Berechnung der Classenanzahl für negative Determinanten abgeleitet (Crelle's Journal LVII).

wo T, U die kleinsten positiven ganzen Zahlen bedeuten, welche der Gleichung

$$T^2 - DU^2 = 1$$

genügen und nach der angegebenen Methode (§. 84) stets gefunden werden können. Hieraus ergeben sich folgende vier Fälle:

V. $D = P$; $P \equiv 1 \pmod{4}$;

$$h = -\left\{2 - \left(\frac{2}{P}\right)\right\} \frac{\Sigma \left(\frac{m}{P}\right) \log \sin \frac{m\pi}{P}}{\log (T + U\sqrt{P})},$$

wo der Buchstabe m alle Werthe zwischen 0 und P durchlaufen muss, die relative Primzahlen zu P sind.

VI. $D = P$; $P \equiv 3 \pmod{4}$;

$$h = -\frac{\Sigma \left(\frac{-1}{m}\right)\left(\frac{m}{P}\right) \log \sin \frac{m\pi}{4P}}{\log (T + U\sqrt{P})},$$

wo der Buchstabe m alle ungeraden Zahlen zwischen 0 und $4P$ durchlaufen muss, die relative Primzahlen zu P sind.

VII. $D = 2P$; $P \equiv 1 \pmod{4}$;

$$h = -\frac{\Sigma \left(\frac{2}{m}\right)\left(\frac{m}{P}\right) \log \sin \frac{m\pi}{8P}}{\log (T + U\sqrt{2P})},$$

wo der Buchstabe m alle ungeraden Zahlen zwischen 0 und $8P$ durchlaufen muss, die relative Primzahlen zu P sind.

VIII. $D = 2P$; $P \equiv 3 \pmod{4}$;

$$h = -\frac{\Sigma \left(\frac{-2}{m}\right)\left(\frac{m}{P}\right) \log \sin \frac{m\pi}{8P}}{\log (T + U\sqrt{2P})},$$

wo der Buchstabe m alle ungeraden Zahlen zwischen 0 und $8P$ durchlaufen muss, die relative Primzahlen zu P sind.

§. 107.

Betrachten wir die so gewonnenen Resultate, so zeigt sich ein wesentlicher Unterschied zwischen den positiven und negati-

ven Determinanten. Während nämlich der Ausdruck für die Classenanzahl bei einer negativen Determinante unmittelbar die Form einer *ganzen* Zahl hat — dass dieselbe zugleich eine *positive* Zahl ist, lässt sich freilich bis jetzt auf elementarem Wege noch nicht nachweisen — so ist dies keineswegs unmittelbar ersichtlich bei den Ausdrücken, welche die Classen-Anzahl für eine positive Determinante darstellen; ja man ist bei der wirklichen Anwendung dieser Formeln auf die Hülfe der logarithmisch-trigonometrischen Tafeln angewiesen, die gewiss als ein der Zahlentheorie sehr fern stehendes Hülfsmittel anzusehen sind. Es ist nun von hohem Interesse, dass die von *Gauss* gegründete Theorie der *Kreistheilung* die Mittel darbietet zu einer solchen Umformung dieser Ausdrücke, welche eine directe Berechnung der Classen-Anzahl gestattet; das wesentliche Resultat besteht darin, dass aus der Theorie der Kreistheilung sich immer eine Auflösung t, u der Pell'schen Gleichung $t^2 - Du^2 = 1$ ableiten lässt, welche aus der kleinsten Auflösung T, U durch Erhebung zur $h$ten Potenz entsteht, so dass

$$(T + U\sqrt{D})^h = t + u\sqrt{D}$$

ist. Dies wollen wir jetzt nachweisen *).

Bedeutet, wie bisher, P eine positive ungerade durch kein Quadrat theilbare Zahl > 1, so zerfällt das System der $\varphi(P)$ Zahlen, die relative Primzahlen zu P und $< P$ sind, bekanntlich (§. 52 I. oder Supplemente I. §. 116) in $\frac{1}{2}\varphi(P)$ Zahlen a und $\frac{1}{2}\varphi(P)$ Zahlen b, für welche respective

$$\left(\frac{a}{P}\right) = +1, \quad \left(\frac{b}{P}\right) = -1$$

ist. Setzen wir ferner, wie früher

$$\theta = e^{\frac{2\pi i}{P}} = \cos\frac{2\pi}{P} + i \sin\frac{2\pi}{P}$$

$$A(x) = \prod (x - \theta^a)$$

$$B(x) = \prod (x - \theta^b),$$

wo die Productzeichen sich auf alle incongruenten a und b beziehen, so ist nach den Supplementen (III. §. 139)

---

*) *Dirichlet: Sur la manière résoudre l'équation* $t^2 - pu^2 = 1$ *au moyen des fonctions circulaires* (Crelle's Journal XVII).

$$2A(x) = Y(x) - i^{\left(\frac{P-1}{2}\right)^2} \sqrt{P} \cdot Z(x)$$
$$2B(x) = Y(x) + i^{\left(\frac{P-1}{2}\right)^2} \sqrt{P} \cdot Z(x)$$

wo $Y(x)$ und $Z(x)$ ganze rationale Functionen von x bedeuten, deren Coefficienten ganze rationale Zahlen sind. Bezeichnet man ferner mit $p, p', p'' \ldots$ die sämmtlichen in $P = pp'p'' \ldots$ aufgehenden Primzahlen, ferner mit μ_1 die positiven, mit μ_2 die negativen Glieder des entwickelten Productes

$$\varphi(P) = (p-1)(p'-1)(p''-1) \ldots = \Sigma \mu_1 - \Sigma \mu_2,$$

so ist

$$A(x)\,B(x) = \frac{\Pi\,(1-x^{\mu_1})}{\Pi\,(1-x^{\mu_2})}.$$

Setzen wir endlich zur Abkürzung

$$\tfrac{1}{2}\varphi(P) = \tau,$$

so ist (Supplemente VII. §. 140)

$$\left.\begin{aligned} A(x) &= x^\tau A\left(\frac{1}{x}\right) \\ B(x) &= x^\tau B\left(\frac{1}{x}\right) \end{aligned}\right\} \text{wenn } P \equiv 1 \pmod 4,$$

und (mit Ausnahme von $P = 3$)

$$\left.\begin{aligned} A(x) &= (-x)^\tau B\left(\frac{1}{x}\right) \\ B(x) &= (-x)^\tau A\left(\frac{1}{x}\right) \end{aligned}\right\} \text{wenn } P \equiv 3 \pmod 4.$$

Auf diesen Sätzen beruhen die oben erwähnten Umformungen, die wir nun für jeden der vier Fälle durchführen wollen. Es sei zunächst

$$D = P \equiv 1 \pmod 4.$$

Dann ist

$$-\Sigma\left(\frac{m}{P}\right)\log\sin\frac{m\pi}{P} = \log\frac{\Pi\sin\frac{b\pi}{P}}{\Pi\sin\frac{a\pi}{P}};$$

verwandelt man jeden Sinus durch die Formel

$$\sin\varphi = \frac{1}{2i}\, e^{-\varphi i}\, (e^{2\varphi i} - 1)$$

und bedenkt, dass

$$\Sigma a - \Sigma b = \Sigma \left(\frac{m}{P}\right) m = \Sigma \left(\frac{P-m}{P}\right)(P-m) = 0$$

ist, so erhält man

$$-\Sigma\left(\frac{m}{P}\right)\log\sin\frac{m\pi}{P} = \log\frac{B(1)}{A(1)}$$

$$= \log\frac{y + z\sqrt{P}}{y - z\sqrt{P}},$$

wo zur Abkürzung die ganzen rationalen Zahlen $Y(1)$ und $Z(1)$ mit y und z bezeichnet sind. Setzt man ferner

$$A(1)\, B(1) = \frac{\Pi\, \mu_1}{\Pi\, \mu_2} = \xi,$$

so findet man leicht (Supplemente §. 138), dass

$$\xi = P \text{ oder } = +1$$

ist; je nachdem P eine Primzahl oder eine zusammengesetzte Zahl ist. Die Zahlen y, z genügen der Gleichung

$$y^2 - Pz^2 = 4\xi,$$

aus welcher folgt, dass, falls P eine Primzahl ist, die Zahl y durch P theilbar ist; man kann daher in jedem Fall

$$\frac{y + z\sqrt{P}}{\sqrt{\xi}} = \alpha + \beta\sqrt{P}$$

setzen, wo α und β zwei ganze Zahlen bedeuten, die der Gleichung

$$\alpha^2 - P\beta^2 = \mp 4$$

genügen, wo das obere oder untere Zeichen gilt, je nachdem P eine Primzahl ist oder nicht. Nun ist

$$-\Sigma\left(\frac{m}{P}\right)\log\sin\frac{m\pi}{P} = \log\frac{B(1)^2}{A(1)B(1)} = \log\left(\frac{\alpha + \beta\sqrt{P}}{2}\right)^2$$

und folglich

$$h = \left\{2 - \left(\frac{2}{P}\right)\right\} \frac{\log\left(\frac{\alpha + \beta\sqrt{P}}{2}\right)^2}{\log(T + U\sqrt{P})}$$

oder, wenn man von den Logarithmen zu den Zahlen übergeht,

$$(T + U\sqrt{P})^h = \left(\frac{\alpha + \beta\sqrt{P}}{2}\right)^{4 - 2\left(\frac{2}{P}\right)}.$$

Ist nun $P \equiv 1 \pmod{8}$, so folgt aus der Gleichung

$$\alpha^2 - P\beta^2 = \mp 4,$$

dass α und β gerade Zahlen sind; setzt man daher

$$\alpha = 2\alpha', \quad \beta = 2\beta',$$

so genügen α', β' der Gleichung

$$\alpha'^2 - P\beta'^2 = \mp 1,$$

und es ist

$$(T + U\sqrt{P})^h = (\alpha' + \beta'\sqrt{P})^2 = t + u\sqrt{P},$$

wo t, u der Gleichung

$$t^2 - Pu^2 = +1$$

genügen.

Ist aber $P \equiv 5 \pmod{8}$, so können α und β auch noch beide gerade Zahlen sein (z. B. wenn $P = 37$), und sie können auch beide ungerade Zahlen sein (z. B. wenn $P = 13$). Setzt man im ersten Fall wieder $\alpha = 2\alpha'$, $\beta = 2\beta'$, so ist

$$\alpha'^2 - P\beta'^2 = \mp 1$$

und

$$(T + U\sqrt{P})^h = (\alpha' + \beta'\sqrt{P})^6 = t + u\sqrt{P},$$

wo offenbar wieder

$$t^2 - Pu^2 = +1$$

ist. Wenn dagegen α und β beide ungerade sind, so ist

$$\left(\frac{\alpha + \beta\sqrt{P}}{2}\right)^3 = \frac{\alpha(\alpha^2 + 3P\beta^2)}{8} + \frac{\beta(3\alpha^2 + P\beta^2)}{8}\sqrt{P}$$
$$= \alpha' + \beta'\sqrt{P},$$

wo α', β' offenbar ganze Zahlen sind, die der Gleichung

$$\alpha'^2 - P\beta'^2 = \mp 1$$

genügen; und dann ist

$$(T + U\sqrt{P})^h = (\alpha' + \beta'\sqrt{P})^2 = t + u\sqrt{P},$$

wo wieder

$$t^2 - Pu^2 = +1$$

ist. Es leuchtet ein, dass der erste oder zweite dieser beiden Fälle eintreten wird, je nachdem die Classenanzahl h durch 3 theilbar ist oder nicht; sind nämlich α und β gerade, so ist

$$\left(\frac{\alpha + \beta\sqrt{P}}{2}\right)^2 = t' + u'\sqrt{P},$$

wo die ganzen Zahlen t', u' der Gleichung

$$t'^2 - Pu'^2 = +1$$

genügen; mithin ist (nach §. 85)

$$t' + u'\sqrt{P} = (T + U\sqrt{P})^n$$

und folglich $h = 3n$; und umgekehrt, ist h theilbar durch 3, so ist

$$\left(\frac{\alpha + \beta\sqrt{P}}{2}\right)^2 = (T + U\sqrt{P})^{\frac{1}{3}h};$$

hieraus folgt aber, dass

$$\frac{\alpha^2 + P\beta^2}{4} \text{ und } \frac{\alpha\beta}{2}$$

ganze Zahlen, also α und β gerade Zahlen sind.

Man erkennt ferner, dass in allen Fällen die Classen-Anzahl ungerade oder gerade sein wird, je nachdem P eine Primzahl oder zusammengesetzt ist; denn wenn h gerade ist, so ist

$$\left(\frac{\alpha + \beta\sqrt{P}}{2}\right)^{2-\left(\frac{2}{P}\right)} = \pm (T + U\sqrt{P})^{\frac{1}{2}h}$$

und folglich

$$\alpha^2 - P\beta^2 = +4,$$

also P zusammengesetzt; und umgekehrt, ist P zusammengesetzt, also $\alpha^2 - P\beta^2 = +4$, so ist

$$\left(\frac{\alpha + \beta\sqrt{P}}{2}\right)^{2-\left(\frac{2}{P}\right)} = t' + u'\sqrt{P},$$

wo t', u' ganze Zahlen bedeuten, die der Gleichung

$$t'^2 - Pu'^2 = +1$$

genügen, folglich (nach §. 85)

$$t' + u'\sqrt{P} = \pm (T + U\sqrt{P})^n$$

und hieraus $h = 2n$.

Endlich mag noch bemerkt werden, dass die beiden mit y und z bezeichneten ganzen Zahlen beide positiv sind; für die Zahl y ist dies unmittelbar einleuchtend; bezeichnet man nämlich mit a' diejenigen Zahlen a, welche $< \frac{1}{2}P$ sind, und ebenso mit b' diejenigen Zahlen b, welche $< \frac{1}{2}P$ sind, so ist

$$y + z\sqrt{P} = 2\prod(1-\theta^{b'})\prod(1-\theta^{-b'})$$

$$y - z\sqrt{P} = 2\prod(1-\theta^{a'})\prod(1-\theta^{-a'})$$

oder einfacher

$$y + z\sqrt{P} = 2^{\tau+1}\prod\left(\sin\frac{b'\pi}{P}\right)^2$$

$$y - z\sqrt{P} = 2^{\tau+1}\prod\left(\sin\frac{a'\pi}{P}\right)^2,$$

woraus unmittelbar folgt, dass y positiv ist. Aus dem oben erhaltenen Resultate

$$(T + U\sqrt{P})^h = \left(\frac{y + z\sqrt{P}}{y - z\sqrt{P}}\right)^{2-\left(\frac{2}{P}\right)},$$

folgt nun weiter, da h eine positive ganze Zahl ist, dass

$$\frac{y + z\sqrt{P}}{y - z\sqrt{P}} > 1,$$

und folglich auch z positiv ist, ein Resultat, das bisher auf anderm Wege noch nicht bewiesen ist.

§. 108.

Ist $D = P \equiv 3 \pmod{4}$, so ist die Summe

$$-\Sigma \left(\frac{-1}{m}\right)\left(\frac{m}{P}\right) \log \sin \frac{m}{4P} = -\tfrac{1}{2}\Sigma \left(\frac{-1}{m}\right)\left(\frac{m}{P}\right) \log \left(\sin \frac{m\pi}{4P}\right)^2$$

zu betrachten, wo m alle ungeraden Zahlen zwischen 0 und $4P$ durchlaufen muss, die relative Primzahlen zu P sind; setzen wir

$$m \equiv 4\alpha + P\gamma \pmod{4P},$$

so muss γ die beiden Werthe $+1$ und -1, ferner α die $\varphi(P)$ Zahlclassen (mod. P) durchlaufen, welche relative Primzahlen zu P enthalten. Dann wird unsere Summe

$$= \tfrac{1}{2}\Sigma (-1)^{\frac{1}{2}(\gamma-1)} \left(\frac{\alpha}{P}\right) \log \left(\sin \left(\frac{\alpha\pi}{P} + \frac{\gamma\pi}{4}\right)\right)^2$$

$$= \tfrac{1}{2}\Sigma \left(\frac{\alpha}{P}\right) \log \left(\frac{\sin\left(\frac{\alpha\pi}{P} + \frac{\pi}{4}\right)}{\sin\left(\frac{\alpha\pi}{P} - \frac{\pi}{4}\right)}\right)^2,$$

oder, wenn man die Sinus wieder durch Exponentialgrössen ausdrückt,

$$= \tfrac{1}{2}\Sigma \left(\frac{\alpha}{P}\right) \log \left(\frac{(\theta^\alpha + i)\, i}{\theta^\alpha - i}\right)^2$$

$$= \tfrac{1}{2}\log \left(\frac{\Pi(\theta^a + i)\,\Pi(\theta^b - i)}{\Pi(\theta^a - i)\,\Pi(\theta^b + i)}\right)^2$$

$$= \tfrac{1}{2}\log \left(\frac{A(-i)\,B(i)}{A(i)\,B(-i)}\right)^2.$$

Da nun $P \equiv 3 \pmod{4}$ ist, so sind die Producte $A(-i)\,B(i)$ und $A(i)\,B(-i)$ positiv, und folglich ist unsere Summe

$$= \log \frac{A(-i)\,B(i)}{A(i)\,B(-i)}.$$

Da ferner, wenn m irgend eine ungerade Zahl bedeutet,

$$\frac{1 - i^m}{1 - i} = i^{\frac{1}{4}(m-1)^2}$$

ist, so findet man

$$A(i)B(i) = \frac{\Pi\,(1-i^{\mu_1})}{\Pi\,(1-i^{\mu_2})} = i^\lambda,$$

wo zur Abkürzung

$$\lambda = \tfrac{1}{4}\{\Sigma\mu_1{}^2 - \Sigma\mu_2{}^2\} - \tfrac{1}{2}\{\Sigma\mu_1 - \Sigma\mu_2\}$$

gesetzt ist; und da

$$\Sigma\mu_1 - \Sigma\mu_2 = (p-1)(p'-1)(p''-1)\ldots$$

und

$$\Sigma\mu_1{}^2 - \Sigma\mu_2{}^2 = (p^2-1)(p'^2-1)(p''^2-1)\ldots$$

so erhält man, wenn P eine zusammengesetzte Zahl ist, $\lambda \equiv 0$ (mod. 4), also

$$A(i)B(i) = 1,\quad A(-i)B(-i) = 1,$$

und wenn P eine Primzahl ist, $\lambda \equiv 1$ (mod 4), also

$$A(i)B(i) = i,\quad A(-i)B(-i) = -i.$$

In beiden Fällen ist daher

$$A(i)B(i)A(-i)B(-i) = +1,$$

und folglich ist unsere obige Summe auch

$$= \log\left(A(-i)^2 B(i)^2\right);$$

wir erhalten daher

$$(T + U\sqrt{P})^h = A(-i)^2 B(i)^2.$$

In unserm Fall ist nun ferner (mit Ausnahme von $P = 3$)

$$A(x) = (-x)^\tau\, B\left(\frac{1}{x}\right),$$

also

$$A(-i) = i^\tau\, B(i)$$

und folglich

$$(T + U\sqrt{P})^h = \mp B(i)^4,$$

wo das obere oder untere Zeichen zu nehmen ist, je nachdem P eine Primzahl (ausser 3) oder zusammengesetzt ist. Aus derselben Relation folgt ferner

$$i^{\tau}\, Y(i) = Y(-i);\quad i^{\tau}\, Z(i) = -Z(-i);$$

ist daher P eine Primzahl, so ist

$$Y(i) = \left(1 + \left(\frac{2}{P}\right) i\right) y$$

$$i\, Z(i) = \left(1 + \left(\frac{2}{P}\right) i\right) z,$$

wo y und z ganze Zahlen bedeuten, also

$$2\, B(i) = \left(1 + \left(\frac{2}{P}\right) i\right) (y + z\sqrt{P})$$

$$2\, A(i) = \left(1 + \left(\frac{2}{P}\right) i\right) (y - z\sqrt{P});$$

und da

$$A(i)\, B(i) = i$$

ist, so genügen y und z der Gleichung

$$y^2 - Pz^2 = \left(\frac{2}{P}\right) 2,$$

woraus folgt, dass y und z ungerade Zahlen sind; man kann daher

$$(y + z\sqrt{P})^2 = 2(\alpha + \beta\sqrt{P})$$

setzen, wo α und β zwei ganze Zahlen bedeuten, die der Gleichung

$$\alpha^2 - P\beta^2 = 1$$

genügen; dann ist

$$B(i)^2 = \left(\frac{2}{P}\right) i\, (\alpha + \beta\sqrt{P})$$

und folglich

$$(T + U\sqrt{P})^h = (\alpha + \beta\sqrt{P})^2.$$

Hieraus ergiebt sich, dass die Classenanzahl h immer $\equiv 2 \pmod{4}$ ist, und ferner, dass y und z immer gleiche Vorzeichen haben.

Ist dagegen P zusammengesetzt, also $\tau = \frac{1}{2}\varphi(P) \equiv 0 \pmod{4}$, und folglich

$$Y(i) = Y(-i),\quad i\,Z(i) = -\, i\,Z(-i),$$

so ist

$$Y(i) = y,\quad i\,Z(i) = z,$$

wo y und z ganze reelle Zahlen bedeuten, und

$$2B(i) = y + z\sqrt{P}, \quad 2A(i) = y - z\sqrt{P}$$

und folglich, da in diesem Fall

$$A(i)B(i) = +1$$

ist,

$$y^2 - Pz^2 = +4;$$

hieraus folgt, dass y und z gerade Zahlen sind; man kann daher

$$B(i) = \alpha + \beta\sqrt{P}$$

setzen, wo α und β ganze reelle Zahlen bedeuten, die der Gleichung

$$\alpha^2 - P\beta^2 = 1$$

genügen, und wir erhalten schliesslich

$$(T + U\sqrt{P})^h = (\alpha + \beta\sqrt{P})^4;$$

hieraus geht hervor, dass h immer durch 4 theilbar ist, und dass α und β gleiche Vorzeichen haben.

Endlich im Fall $P = 3$ ist

$$Y(x) = 2x + 1, \quad Z(x) = 1$$

und folglich

$$2B(i) = 1 + (2 + \sqrt{3})\,i, \quad 2A(-i) = 1 - (2 + \sqrt{3})\,i$$

$$4A(-i)B(i) = 8 + 4\sqrt{3} = 4(2 + \sqrt{3}) = 4(T + U\sqrt{P})$$

und also $h = 2$.

§. 109.

Ist $D = 2P \equiv 2 \pmod{8}$, so ist folgende Summe zu betrachten

$$-\Sigma\left(\frac{2}{m}\right)\left(\frac{m}{P}\right)\log\sin\frac{m\pi}{8P} =$$

$$-\tfrac{1}{2}\Sigma\left(\frac{2}{m}\right)\left(\frac{m}{P}\right)\log\left(\sin\frac{m\pi}{8P}\right)^2,$$

wo der Buchstabe m alle zwischen 0 und $8P$ liegenden Zahlen

durchlaufen muss, die relative Primzahlen zu $8P$ sind. Lässt man γ die vier Werthe 1, 3, 5, 7 (mod. 8) und α die $\varphi(P)$ nach dem Modulus P incongruenten Werthe durchlaufen, die relative Primzahlen zu P sind, so kann man

$$m \equiv 8\alpha + P\gamma \pmod{8P}$$

setzen; dann wird unsere Summe

$$= -\tfrac{1}{2}\Sigma\left(\frac{2}{\gamma}\right)\left(\frac{\alpha}{P}\right)\log\left(\sin\left(\frac{\alpha\pi}{P}+\frac{\gamma\pi}{8}\right)\right)^2;$$

fasst man jedesmal die vier Glieder zusammen, welche demselben Werth α und den sämmtlichen vier Werthen von γ entsprechen, so wird die Summe

$$= \tfrac{1}{2}\Sigma\left(\frac{\alpha}{P}\right)\log\left(\frac{\sin\left(\frac{\alpha\pi}{P}+\frac{3\pi}{8}\right)\sin\left(\frac{\alpha\pi}{P}+\frac{5\pi}{8}\right)}{\sin\left(\frac{\alpha\pi}{P}+\frac{\pi}{8}\right)\sin\left(\frac{\alpha\pi}{P}+\frac{7\pi}{8}\right)}\right)^2;$$

drückt man ferner die Sinus durch Exponentialfunctionen aus und setzt zur Abkürzung, wie früher,

$$e^{1/4\pi i} = \frac{1+i}{\sqrt{2}} = j,$$

so nimmt die Summe folgende Gestalt an:

$$\tfrac{1}{2}\Sigma\left(\frac{\alpha}{P}\right)\log\left(\frac{(j^3-\theta^\alpha)\,(j^5-\theta^\alpha)}{(j-\theta^\alpha)\,(j^7-\theta^\alpha)}\right)^2$$

$$= \tfrac{1}{2}\log\left(\frac{A(j^3)\,A(j^5)\,B(j)\,B(j^7)}{A(j)\,A(j^7)\,B(j^3)\,B(j^5)}\right)^2.$$

Da nun $P \equiv 1 \pmod{4}$ ist, so leuchtet ein, dass die Producte

$$A(j)\,A(j^7),\quad A(j^3)\,A(j^5),\quad B(j)\,B(j^7),\quad B(j^3)\,B(j^5)$$

positive Werthe haben, und folglich ist unsere Summe

$$= \log\frac{A(j^3)A(j^5)\,B(j)\,B(j^7)}{A(j)A(j^7)B(j^3)B(j^5)}.$$

Da ferner, wenn m irgend eine ungerade Zahl bedeutet,

$$\frac{(1-j^m)\,(1-j^{3m})}{(1-j)\,(1-j^3)} = \left(\frac{-2}{m}\right),$$

so ist

$$A(j)B(j)A(j^3)B(j^3) = \frac{\Pi(1-j^{\mu_1})(1-j^{3\mu_1})}{\Pi(1-j^{\mu_2})(1-j^{3\mu_2})} =$$

$$= \frac{\Pi\left(\frac{-2}{\mu_1}\right)}{\Pi\left(\frac{-2}{\mu_2}\right)} = \frac{\left(\frac{-2}{\Pi\mu_1}\right)}{\left(\frac{-2}{\Pi\mu_2}\right)};$$

und da (Supplemente §. 138)

$$\Pi\mu_1 = P\cdot\Pi\mu_2 \text{ oder } = \Pi\mu_2$$

ist, je nachdem P eine Primzahl oder eine zusammengesetzte Zahl, so erhält man entsprechend

$$A(j)B(j)A(j^3)B(j^3) = \left(\frac{-2}{P}\right) \text{ oder } = 1.$$

Da ferner

$$A(j^5)B(j^5)A(j^7)B(j^7)$$

offenbar denselben Werth hat, so ist unsere Summe auch

$$= \log[A(j^3)A(j^5)B(j)B(j^7)]^2$$

und folglich

$$(T + U\sqrt{2P})^h = [A(j^3)A(j^5)B(j)B(j^7)]^2.$$

Aus

$$A(x) = x^\tau A\left(\frac{1}{x}\right),\ B(x) = x^\tau B\left(\frac{1}{x}\right)$$

folgt ferner

$$A(j^5) = j^{5\tau} A(j^3),\quad B(j^7) = j^{7\tau} B(j),$$

also

$$(T + U\sqrt{2P})^h = [A(j^3)B(j)]^4.$$

Aus denselben Gleichungen, d. h. aus den Gleichungen

$$Y(x) = x^\tau Y\left(\frac{1}{x}\right),\ Z(x) = x^\tau Z\left(\frac{1}{x}\right)$$

folgt ferner, dass man

$$Y(j) = j^{\frac{1}{2}\tau}\{y' + y''(j - j^3)\},\ Z(j) = j^{\frac{1}{2}\tau}\{z' + z''(j - j^3)\}$$

setzen kann, wo y', y'', z', z'' ganze rationale Zahlen bedeuten; da ferner

$$j - j^3 = \sqrt{2}$$

ist, so erhält man, wenn man

$$\alpha = (-1)^{\frac{1}{2}\tau}\{y'^2 - 2y''^2 - P(z'^2 - 2z''^2)\}$$
$$\beta = (-1)^{\frac{1}{2}\tau}\, 2(y'z'' - y''z')$$

setzt,

$$4A(j^3)B(j) = \alpha + \beta\sqrt{2P},$$
$$4A(j)B(j^3) = \alpha - \beta\sqrt{2P},$$

wo α und β ganze Zahlen sind, die der Gleichung

$$\alpha^2 - 2P\beta^2 = \pm 16$$

genügen, in welcher das untere Zeichen nur dann zu nehmen ist, wenn P eine Primzahl und zugleich $\equiv 5 \pmod{8}$ ist. Aus dieser Gleichung folgt leicht, dass α und β durch 4 theilbar sind; man kann daher

$$A(j^3)B(j) = y + z\sqrt{2P}$$

setzen, wo y und z ganze Zahlen sind, die der Gleichung

$$y^2 - 2Pz^2 = \pm 1$$

genügen, und dann ist

$$(T + U\sqrt{2P})^h = (y + z\sqrt{2P})^4.$$

Hieraus folgt, dass $h \equiv 2 \pmod{4}$, falls P eine Primzahl von der Form $8n + 5$, und in allen andern Fällen $h \equiv 0 \pmod{4}$ ist.

Im Fall $P = 1$, also $D = 2$, welcher bisher stillschweigend ausgenommen ist, erhält man unmittelbar

$$-\Sigma\left(\frac{2}{m}\right)\left(\frac{m}{P}\right)\log\sin\frac{m\pi}{8P} = \log\frac{\sin\frac{3\pi}{8}\sin\frac{5\pi}{8}}{\sin\frac{\pi}{8}\sin\frac{7\pi}{8}}$$

$$= \log \frac{(1-j^3)(1-j^5)}{(1-j)(1-j^7)} = \log (1+\sqrt{2})^2 = \log (3+2\sqrt{2})$$
$$= \log (T + U\sqrt{2P}),$$

und folglich $h = 1$.

§. 110.

Ist $D = 2P \equiv 6 \pmod{8}$, so erhält man ganz ähnlich wie im vorigen Fall

$$-\Sigma \left(\frac{-2}{m}\right)\left(\frac{m}{P}\right) \log \sin \frac{m\pi}{8P}$$
$$= \log \frac{A(j^5)A(j^7)B(j)B(j^3)}{A(j)A(j^3)B(j^5)B(j^7)},$$

und da

$$A(j)B(j)A(j^3)B(j^3) = A(j^5)B(j^5)A(j^7)B(j^7)$$
$$= \left(\frac{-2}{P}\right) \text{ oder } = 1$$

ist, je nachdem P Primzahl oder zusammengesetzt ist, so erhält man

$$(T + U\sqrt{2P})^h = [A(j^5)A(j^7)B(j)B(j^3)]^2.$$

Mit Ausnahme des Falls $P = 3$ ist ferner

$$A(x) = (-x)^\tau B\left(\frac{1}{x}\right),$$

folglich

$$A(j^5) = (-1)^\tau j^{5\tau} B(j^3)$$
$$A(j^7) = (-1)^\tau j^{7\tau} B(j),$$

also

$$A(j^5)A(j^7) = (-1)^\tau B(j)B(j^3),$$

und folglich

$$(T + U\sqrt{2P})^h = [B(j)B(j^3)]^4.$$

Ist nun P eine Primzahl (> 3), also $\tau = \frac{1}{2}(P-1)$ ungerade, so folgt aus

$$Y(x) = -x^\tau \, Y\left(\frac{1}{x}\right)$$
$$Z(x) = +x^\tau \, Z\left(\frac{1}{x}\right),$$

dass man

$$Y(j^\tau) = y'(1-j) + y''(j^2+j^3)$$
$$Z(j^\tau) = z'(1+j) + z''(j^2-j^3)$$

setzen kann, wo y', y'', z', z'' ganze rationale Zahlen bedeuten. Setzt man ferner zur Abkürzung

$$\alpha = (-y'^2 + 2y'y'' + y''^2) - P(z'^2 - 2z'z'' - z''^2)$$
$$\beta = 4y'z' + 4y''z'',$$

so erhält man

$$4B(j)\,B(j^3) = \alpha(j^\tau + j^{3\tau}) + \beta i \sqrt{P}$$
$$4A(j)\,A(j^3) = \alpha(j^\tau + j^{3\tau}) - \beta i \sqrt{P};$$

da nun in unserm Fall

$$A(j)\,B(j)\,A(j^3)\,B(j^3) = -\left(\frac{2}{P}\right),$$

und ausserdem

$$j^\tau + j^{3\tau} = \left(\frac{-2}{\tau}\right) i \sqrt{2}$$

ist, so müssen die beiden Zahlen α, β der Gleichung

$$2\alpha^2 - P\beta^2 = 16\left(\frac{2}{P}\right)$$

genügen, woraus folgt, dass sie beide durch 4 theilbar sein müssen; man kann daher

$$\alpha = 4\left(\frac{-2}{\tau}\right) y, \quad \beta = 4z$$

setzen, wo die ganzen Zahlen y und z der Gleichung

$$2y^2 - Pz^2 = \left(\frac{2}{P}\right)$$

genügen, und dann ist

$$(T + U\sqrt{2P})^h = (y\sqrt{2} + z\sqrt{P})^4 = (y_1 + z_1\sqrt{2P})^2,$$

wo die ganzen Zahlen

$$y_1 = 2y^2 + Pz^2, \quad z_1 = 2yz$$

der Gleichung

$$y_1^2 - 2Pz_1^2 = 1$$

genügen. Hieraus folgt, dass $h \equiv 2 \pmod{4}$ ist.

Ist dagegen P eine zusammengesetzte Zahl, also $\tau \equiv 0 \pmod{4}$, und

$$Y(x) = +x^\tau \; Y\left(\frac{1}{x}\right)$$

$$Z(x) = -x^\tau \; Z\left(\frac{1}{x}\right),$$

so kann man

$$Y(j) = j^{\frac{1}{2}\tau} \, \{y' + y''(j - j^3)\}$$

$$j^2 Z(j) = j^{\frac{1}{2}\tau} \, \{z' + z''(j - j^3)\}$$

setzen, wo y', y'', z', z'' ganze rationale Zahlen bedeuten. Setzt man dann

$$\alpha = y'^2 - Pz'^2 - 2y''^2 + 2Pz''^2,$$

$$\beta = 2(y'z'' - y''z'),$$

so findet man

$$4B(j)B(j^3) = \alpha + \beta\sqrt{2P}$$

$$4A(j)A(j^3) = \alpha - \beta\sqrt{2P},$$

und da jetzt

$$A(j)B(j)A(j^3)B(j^3) = +1$$

ist, so genügen die Zahlen α, β der Gleichung

$$\alpha^2 - 2P\beta^2 = 16;$$

hieraus folgt, dass man

$$\alpha = 4y, \quad \beta = 4z$$

setzen kann, wo y, z ganze Zahlen bedeuten, die der Gleichung

$$y^2 - 2Pz^2 = 1$$

genügen, und es ist

$$(T + U\sqrt{2P})^h = (y + z\sqrt{2P})^4,$$

woraus folgt, dass h immer durch 4 theilbar ist.

Endlich im Fall $P = 3$ ist

$$Y(x) = 2x + 1, \quad Z(x) = 1,$$

also

$$2B(j) = 2j + 1 + i\sqrt{3}, \quad 2B(j^3) = 2j^3 + 1 + i\sqrt{3},$$
$$2A(j^5) = 2j^5 + 1 - i\sqrt{3}, \quad 2A(j^7) = 2j^7 + 1 - i\sqrt{3},$$

und folglich

$$B(j)A(j^5) = \frac{1-i}{\sqrt{2}}(\sqrt{2} + \sqrt{3})$$

$$B(j^3)A(j^7) = \frac{1+i}{\sqrt{2}}(\sqrt{2} + \sqrt{3})$$

$$A(j^5)A(j^7)B(j)B(j^3) = (\sqrt{2} + \sqrt{3})^2 = 5 + 2\sqrt{6}$$

und

$$(T + U\sqrt{2P})^h = (\sqrt{2} + \sqrt{3})^4 = (5 + 2\sqrt{6})^2,$$

also $h = 2$.

SUPPLEMENTE.

I. Ueber einige Sätze von Gauss aus der Theorie der Kreistheilung.

§. 111.

Wir schicken zunächst ein Lemma aus der Theorie der Fourier'schen Reihen voraus, deren Glieder nach den Cosinus der successiven Vielfachen eines Winkels fortschreiten; es wird in derselben nachgewiesen *), dass für alle Werthe von x zwischen $x = 0$ und $x = \pi$ mit Einschluss dieser Grenzen stets

$$\varphi(x) = \tfrac{1}{2} a_0 + a_1 \cos x + a_2 \cos 2x + a_3 \cos 3x + \cdots$$

ist, wenn $\varphi(x)$ eine innerhalb dieses Intervalles endliche und stetige Function bedeutet, und die Coefficienten $a_0, a_1, a_2 \ldots$ durch die Gleichung

$$a_s = \frac{2}{\pi} \int_0^\pi \varphi(x) \cos sx\, dx$$

bestimmt werden. Hieraus folgt für $x = 0$

$$\pi \varphi(0) = \sum_{-\infty}^{+\infty} \int_0^\pi \varphi(x) \cos sx\, dx,$$

wo das Summenzeichen sich auf den Buchstaben s bezieht, für welchen Null und alle ganzen positiven und negativen Zahlwerthe einzusetzen sind. Auf diesen der genannten Theorie entlehnten Satz stützen wir uns im Folgenden.

---

*) *Dirichlet*: *Sur la convergence des séries etc.* (Crelle's Journal IV); derselbe Beweis ist vereinfacht in Dove's Repertorium der Physik I.

Zunächst verallgemeinern wir denselben, indem wir das Integral

$$\int_0^{2h\pi} f(x) \cos sx\, dx$$

betrachten, in welchem h eine positive ganze Zahl, s eine positive oder negative ganze Zahl, und $f(x)$ eine innerhalb des Integrationsgebietes endliche und stetige Function bedeutet. Man kann dasselbe in $2h$ Integrale von der Form

$$\int_{r\pi}^{(r+1)\pi} f(x) \cos sx\, dx$$

zerlegen, wo für r der Reihe nach die Zahlen 0, 1, 2 . . . bis $2h - 1$ zu setzen sind; je nachdem r eine gerade oder ungerade Zahl ist, ersetzen wir die Integrationsvariabele x durch $r\pi + x$, oder durch $(r + 1)\pi - x$; dadurch geht das vorstehende Integral in

$$\int_0^{\pi} f(r\pi + x) \cos sx\, dx, \text{ oder in } \int_0^{\pi} f((r + 1)\pi - x) \cos sx\, dx$$

über, und hieraus ergiebt sich

$$\int_0^{2h\pi} f(x) \cos sx\, dx = \int_0^{\pi} \varphi(x) \cos sx\, dx,$$

wenn zur Abkürzung

$$\varphi(x) = \left\{\begin{matrix} f(x) + f(2\pi - x) + f(2\pi + x) + f(4\pi - x) \\ + \cdots + f(2(h-1)\pi + x) + f(2h\pi - x) \end{matrix}\right\}$$

gesetzt wird. Wenden wir nun auf diese Function $\varphi(x)$ das vorstehende Lemma an, so erhalten wir den Satz

$$2\pi\{\tfrac{1}{2}f(0) + f(2\pi) + f(4\pi) + \cdots + f(2(h-1)\pi) + \tfrac{1}{2}f(2h\pi)\}$$
$$= \sum_{-\infty}^{+\infty} \int_0^{2h\pi} f(x) \cos sx\, dx.$$

§. 112.

Wir beschäftigen uns nun mit den beiden folgenden bestimmten Integralen

$$p = \int_{-\infty}^{+\infty} \cos(x^2)\, dx,\ q = \int_{-\infty}^{+\infty} \sin(x^2)\, dx;$$

dass dieselben wirklich bestimmte endliche Werthe besitzen, obgleich die Functionen unter den Integralzeichen für unendlich grosse Werthe von x nicht unendlich klein werden, erkennt man leicht durch die Transformationen

$$p = 2\int_0^\infty \cos(x^2)\, dx = \int_0^\infty \frac{\cos y}{\sqrt{y}}\, dy$$

$$g = 2\int_0^\infty \sin(x^2)\, dx = \int_0^\infty \frac{\sin y}{\sqrt{y}}\, dy;$$

denn zerlegt man das ganze unendliche Integrationsgebiet der positiven Variabeln y in solche Intervalle, in deren jedem die unter dem Integralzeichen befindliche Function ihr Zeichen nicht ändert, so ergiebt sich, dass die Bestandtheile, welche diesen Intervallen entsprechen, eine unendliche Reihe bilden, deren Glieder abwechselnde Zeichen haben und dem absoluten Werth nach beständig und zwar ins Unendliche abnehmen; woraus folgt, dass diese Reihe, sowohl bei dem Integrale p, wie bei q, eine convergente ist. Für unsern Zweck genügt dieser Nachweis der Endlichkeit von p und q; die numerischen Werthe dieser Integrale werden sich von selbst aus der folgenden Untersuchung ergeben.

Wir können beide Integrale in ein einziges zusammenfassen; bezeichnen wir nämlich mit δ irgend einen Winkel, und setzen wir zur Abkürzung

$$p\cos\delta - q\sin\delta = \Delta,$$

so ist

$$\Delta = \int_{-\infty}^{+\infty} \left\{\cos\delta\cos(x^2) - \sin\delta\sin(x^2)\right\} dx$$

oder

$$\Delta = \int\limits_{-\infty}^{+\infty} \cos(\delta + x^2)\, dx;$$

bezeichnen wir ferner mit α eine beliebige positive Constante und mit $\sqrt{\alpha}$ die *positiv* genommene Quadratwurzel aus α, so ergiebt sich, wenn man die Integrationsvariabele x durch $x\sqrt{\alpha}$ ersetzt, folgende Gleichung

$$\frac{\Delta}{\sqrt{\alpha}} = \int\limits_{-\infty}^{+\infty} \cos(\delta + \alpha x^2)\, dx$$

(wäre $\sqrt{\alpha}$ negativ, so müsste man auch in dem Integrale rechter Hand die beiden Grenzen mit einander vertauschen). Wir führen nun eine zweite positive Constante β ein, und zerlegen das vorstehende Integral in unendlich viele Bestandtheile von der Form

$$\int\limits_{s\beta}^{(s+1)\beta} \cos(\delta + \alpha x^2)\, dx,$$

wo für s successive alle ganzen Zahlen von $-\infty$ bis $+\infty$ einzusetzen sind; in jedem einzelnen solchen Integrale ersetzen wir die Integrationsvariabele x durch $s\beta + x$, wodurch es in das folgende übergeht

$$\int\limits_{0}^{\beta} \cos(\delta + \alpha s^2\beta^2 + 2\alpha s\beta x + \alpha x^2)\, dx.$$

Wir verfügen nun über die beiden bis jetzt ganz willkürlichen positiven Constanten α und β folgendermaassen: unter m verstehen wir irgend eine positive ganze Zahl, und setzen $\alpha\beta^2 = 2m\pi$, $2\alpha\beta = 1$, d. h. also

$$\beta = 4m\pi,\ \alpha = \frac{1}{8m\pi}.$$

Da nun s eine ganze Zahl ist, so wird

$$\cos(\delta + \alpha s^2\beta^2 + 2\alpha s\beta x + \alpha x^2) = \cos(\delta + sx + \alpha x^2)$$

$$= \cos\left(\delta + \frac{x^2}{8m\pi}\right)\cos sx - \sin\left(\delta + \frac{x^2}{8mx}\right)\sin sx,$$

und folglich

$$\int_{s\beta}^{(s+1)\beta} \cos(\delta + \alpha x^2)\, dx =$$

$$\int_0^{4m\pi} \cos\left(\delta + \frac{x^2}{8m\pi}\right) \cos sx\, dx - \int_0^{4m\pi} \sin\left(\delta + \frac{x^2}{8m\pi}\right) \sin sx\, dx.$$

Das zweite Integral rechter Hand, welches unter dem Integralzeichen den Factor $\sin sx$ enthält, verschwindet offenbar für $s = 0$, und nimmt für je zwei gleiche, aber entgegengesetzte Werthe von s ebenfalls gleiche, aber entgegengesetzte Werthe an. Summiren wir daher den vorstehenden Ausdruck für alle ganzen Zahlwerthe s von $-\infty$ bis $+\infty$, so ergiebt sich

$$\frac{\Delta}{\sqrt{\alpha}} = \Delta\sqrt{8m\pi} = \sum_{-\infty}^{+\infty} \int_0^{4m\pi} \cos\left(\delta + \frac{x^2}{8m\pi}\right) \cos sx\, dx.$$

Die rechte Seite dieser Gleichung ist nun genau so gebaut wie in dem Satze am Schlusse des vorhergehenden Paragraphen; setzen wir zur Abkürzung

$$f(x) = \cos\left(\delta + \frac{x^2}{8m\pi}\right),$$

so erhalten wir

$$\Delta\sqrt{8m\pi} = 2\pi\,\{\tfrac{1}{2}f(0) + f(2\pi) + \cdots + f(2(2m-1)\pi) + \tfrac{1}{2}f(4m\pi)\},$$

wo links die Quadratwurzel

$$\sqrt{8m\pi} = \frac{1}{\sqrt{\alpha}}$$

positiv zu nehmen ist. Nun ist ferner, wenn s irgend eine ganze Zahl bedeutet,

$$f(4m\pi + 2s\pi) = f(2s\pi),$$

also

$$f(2s\pi) = \tfrac{1}{2}f(2s\pi) + \tfrac{1}{2}f(4m\pi + 2s\pi);$$

mithin kann die in den Parenthesen eingeschlossene Summe auch in die Form

$$\tfrac{1}{2}\sum f(2s\pi)$$

gebracht werden, wo der Buchstabe s die Zahlen

$$0, 1, 2 \ldots (4m - 1)$$

oder irgend ein anderes vollständiges Restsystem in Bezug auf den Modul $4m$ durchlaufen muss; und man erhält also

$$\Delta \sqrt{8m\pi} = \pi \sum \cos\left(\delta + s^2 \frac{\pi}{2m}\right).$$

Setzt man ferner $4m = n$, so dass n irgend eine ganze positive, aber durch 4 theilbare Zahl bedeutet, und bezeichnet man mit $\sqrt{n}$ und $\sqrt{\frac{1}{2}\pi}$ die *positiv* genommenen Quadratwurzeln aus n und $\frac{1}{2}\pi$, so nimmt die Gleichung folgende Gestalt an

$$\Delta \sqrt{n} = \sqrt{\tfrac{1}{2}\pi} \cdot \sum \cos\left(\delta + s^2 . \frac{2\pi}{n}\right),$$

wo s ein vollständiges Restsystem in Bezug auf den Modul n durchlaufen muss. Nun ist

$$\Delta = p \cos \delta - q \sin \delta,$$

wo p, q die obigen Integralwerthe bedeuten, die von n und dem willkürlichen δ ganz unabhängig sind; wir können daher p und q durch eine specielle Annahme für n, am einfachsten durch die Annahme $n = 4$ bestimmen; auf diese Weise erhalten wir

$$2(p \cos \delta - q \sin \delta) = 2(\cos \delta - \sin \delta) \sqrt{\tfrac{1}{2}\pi},$$

und in Folge der Willkürlichkeit von δ

$$p = q = \sqrt{\tfrac{1}{2}\pi}.$$

Nachdem so die Werthe von p und q gefunden sind, nimmt unsere obige Gleichung folgende Gestalt an

$$\sum \cos\left(\delta + s^2 \frac{2\pi}{n}\right) = (\cos \delta - \sin \delta) \sqrt{n}$$

und sie zerfällt in die beiden folgenden:

$$\sum \cos\left(s^2 \frac{2\pi}{n}\right) = \sqrt{n}$$

$$\sum \sin\left(s^2 \frac{2\pi}{n}\right) = \sqrt{n};$$

hierin bedeutet also n jede beliebige ganze positive Zahl, welche

$\equiv 0 \pmod{4}$ ist, und $\sqrt{n}$ die *positiv* genommene Quadratwurzel aus n. Bezeichnet man zur Abkürzung $\sqrt{-1}$ mit i, und, wie gewöhnlich, mit e die Basis des natürlichen Logarithmensystems, so kann man beide Gleichungen in die eine Gleichung

$$\sum e^{s^2 \cdot \frac{2\pi i}{n}} = (1 + i)\sqrt{n}$$

zusammenziehen, in welcher der Buchstabe s ein vollständiges Restsystem (mod. n) zu durchlaufen hat.

§. 113.

Wir wollen jetzt Summen betrachten, welche die vorstehende als speciellen Fall enthalten; wir bezeichnen mit n irgend eine ganze positive Zahl, mit h irgend eine positive oder negative ganze Zahl, und setzen zur Abkürzung

$$\sum e^{s^2 \frac{2h\pi i}{n}} = \varphi(h, n),$$

wo der Summationsbuchstabe s irgend ein vollständiges Restsystem in Bezug auf den Modulus n durchlaufen muss.

Mit Hülfe dieser Bezeichnungsweise können wir den im vorigen Paragraphen bewiesenen Satz in folgender Weise ausdrücken:

$$\varphi(1, n) = (1 + i)\sqrt{n}, \quad \text{wenn } n \equiv 0 \pmod{4}.$$

Wir wollen nun folgende drei Eigenschaften des Ausdrucks $\varphi(h, n)$ allgemein beweisen:

1) Ist $h \equiv h' \pmod{n}$, so ist

$$\varphi(h, n) = \varphi(h', n);$$

dies folgt unmittelbar daraus, dass für jeden ganzzahligen Werth von s stets

$$e^{s^2 \frac{2h\pi i}{n}} = e^{s^2 \frac{2h'\pi i}{n}}$$

ist.

2) Ist a relative Primzahl gegen n, so ist

$$\varphi(ha^2, n) = \varphi(h, n);$$

denn es ist

$$\varphi(ha^2, n) = \sum e^{(as)^2 \frac{2h\pi i}{n}},$$

und wenn s ein vollständiges Restsystem nach dem Modul n durchläuft, so gilt (nach §. 18) dasselbe von as.

3) Sind m, n irgend zwei relative Primzahlen, und beide positiv, so ist

$$\varphi(hm, n)\, \varphi(hn, m) = \varphi(h, mn).$$

Es ist nämlich

$$\varphi(hm, n) = \sum e^{s^2 \frac{2hm\pi i}{n}}$$

$$\varphi(hn, m) = \sum e^{t^2 \frac{2hn\pi i}{m}},$$

wo die Buchstaben s, t vollständige Restsysteme resp. in Bezug auf die Moduln n, m durchlaufen müssen; und folglich ist

$$\varphi(hm, n)\, \varphi(hn, m) = \sum e^{\left(\frac{ms^2}{n} + \frac{nt^2}{m}\right) 2h\pi i},$$

wo das Summenzeichen rechter Hand sich auf alle mn Combinationen jedes Werthes von s mit jedem Werthe von t bezieht. Da nun

$$\frac{ms^2}{n} + \frac{nt^2}{m} = \frac{(ms + nt)^2}{mn} - 2st$$

ist, und alle Multipla von $2\pi i$ im Exponenten fortgelassen werden können, so ist auch

$$\varphi(hm, n)\, \varphi(hn, m) = \sum e^{(ms+nt)^2 \frac{2h\pi i}{mn}},$$

wo das Summenzeichen sich wieder auf sämmtliche Werthe von s und t bezieht. Setzt man nun

$$ms + nt = r,$$

so nimmt r, wenn s und t alle ihnen zukommenden Werthe durchlaufen, im Ganzen mn Werthe an, und zwar sind diese alle incongruent nach dem Modulus mn; denn aus

$$ms + nt \equiv ms' + nt' \pmod{mn}$$

folgt

$$ms \equiv ms' \pmod{n}, \quad nt \equiv nt' \pmod{m}$$

und folglich, da m und n relative Primzahlen sind,

$$s \equiv s' \text{ (mod. } n), \quad t \equiv t' \text{ (mod. } m);$$

d. h. die Zahl r nimmt nur dann Werthe an, welche nach dem Modul mn congruent sind, wenn die Werthe von s congruent nach dem Modul n, und gleichzeitig die Werthe von t congruent nach dem Modul m sind. Den mn verschiedenen Combinationen von s und t correspondiren daher mn Werthe von r, welche nach dem Modul mn incongruent sind, und folglich bilden diese Werthe von r ein vollständiges Restsystem nach dem Modul mn. Es ist folglich

$$\varphi(hm, n)\, \varphi(hn, m) = \sum e^{r^2 \frac{2h\pi i}{mn}} = \varphi(h, mn),$$

was zu beweisen war.

§. 114.

Mit Hülfe dieser Sätze können wir nun den Werth von $\varphi(1, n)$, welcher für den Fall, dass $n \equiv 0$ (mod. 4) ist, schon in §. 112 gefunden ist, auch für alle andern Werthe der Zahl n bestimmen. Ist zunächst n irgend eine *ungerade* Zahl, so nehmen wir in dem letzten Satze des vorigen Paragraphen

$$h = 1, \quad m = 4,$$

und erhalten

$$\varphi(4, n)\, \varphi(n, 4) = \varphi(1, 4n);$$

nun ist nach dem zweiten Satz des vorigen Paragraphen

$$\varphi(4, n) = \varphi(2^2, n) = \varphi(1, n);$$

ferner ist

$$\varphi(n, 4) = 2(1 + i^n),$$

und nach dem in §. 112 gefundenen Resultat

$$\varphi(1, 4n) = (1 + i) \sqrt{4n} = 2(1 + i) \sqrt{n},$$

wo die Quadratwurzel $\sqrt{n}$ wieder positiv genommen werden muss. Hieraus ergiebt sich also

$$\varphi(1, n) . 2(1 + i^n) = 2(1 + i) \sqrt{n}$$

oder

$$\varphi(1, n) = \frac{1+i}{1+i^n} \sqrt{n};$$

je nachdem nun $n \equiv 1$ oder $\equiv 3$ (mod. 4) ist, wird

$$i^n = i, \quad \text{oder} = -i$$

und folglich

$$\frac{1+i}{1+i^n} = 1, \quad \text{oder} = \frac{1+i}{1-i} = i,$$

also

$$\varphi(1, n) = \sqrt{n}, \quad \text{oder} = i \sqrt{n};$$

diese beiden Fälle lassen sich aber in die eine Formel

$$\varphi(1, n) = i^{1/4 (n-1)^2} \sqrt{n}$$

zusammenfassen.

Ist endlich n durch 2, aber nicht durch 4 theilbar, also das Doppelte einer ungeraden Zahl, so setzen wir in dem dritten Satz des vorigen Paragraphen $h = 1$, ferner $m = 2$, und $\frac{1}{2} n$ statt n, wodurch allen Bedingungen desselben Genüge geschieht, und erhalten

$$\varphi(2, \tfrac{1}{2} n)\, \varphi(\tfrac{1}{2} n, 2) = \varphi(1, n);$$

nun ist aber

$$\varphi(\tfrac{1}{2} n, 2) = 0$$

und folglich auch

$$\varphi(1, n) = 0.$$

Wir wollen die so gewonnenen Resultate in folgender Tabelle zusammenfassen:

$$\varphi(1, n) = (1 + i) \sqrt{n}, \text{ wenn } n \equiv 0 \text{ (mod. 4)}$$

$$\varphi(1, n) = i^{1/4 (n-1)^2} \sqrt{n}, \text{ wenn } n \equiv 1 \text{ (mod. 2)}$$

$$\varphi(1, n) = 0 \qquad , \text{ wenn } n \equiv 2 \text{ (mod. 4)}.$$

Von der grössten Wichtigkeit ist aber die Bemerkung, dass die in den beiden ersten Formeln vorkommende Quadratwurzel $\sqrt{n}$ durchaus *positiv* genommen werden muss, wie es sich bei der Untersuchung in §. 112. herausgestellt hat. Ohne diese nähere Bestimmung würden die vorstehenden Sätze sich auf viel einfachere Art

beweisen lassen; *Gauss* wurde zuerst in seiner Theorie der Kreistheilung auf die Betrachtung solcher Summen geführt *); es ergiebt sich dort ohne Schwierigkeit der Werth des Quadrates derselben; der viel tiefer liegenden Bestimmung des Vorzeichens der Quadratwurzel widmete er aber eine besondere Abhandlung **), in welcher er auf einem, von dem hier (in §. 112) eingeschlagenen gänzlich verschiedenen Wege, nämlich durch rein algebraische Zerlegung dieser Summen in Producte, vollständig zum Ziele gelangte.

§ 115.

Wir suchen nun den Werth von $\varphi(h, n)$ auch für beliebige Werthe von h zu bestimmen, beschränken uns dabei aber auf den Fall, dass n eine ungerade Primzahl ist, die wir mit p bezeichnen wollen. Bezeichnen wir mit α die sämmtlichen $\frac{1}{2}(p-1)$ incongruenten quadratischen Reste von p, mit β die $\frac{1}{2}(p-1)$ quadratischen Nichtreste, so ist (nach §. 33)

$$\varphi(h, p) = \Sigma\, e^{s^2 \frac{2h\pi i}{p}} = 1 + 2\, \Sigma\, e^{\alpha \frac{2h\pi i}{p}};$$

da ferner

$$1 + \Sigma\, e^{\alpha \frac{2h\pi i}{p}} + \Sigma\, e^{\beta \frac{2h\pi i}{p}} = \Sigma\, e^{s \frac{2h\pi i}{p}} = 0$$

ist, sobald h nicht durch p theilbar ist, so können wir für diesen Fall mit Benutzung des Legendre'schen Symbols

$$\varphi(h, p) = \Sigma\, e^{\alpha \frac{2h\pi i}{p}} - \Sigma\, e^{\beta \frac{2h\pi i}{p}} = \Sigma \left(\frac{s}{p}\right) e^{s \frac{2h\pi i}{p}}$$

setzen, wo s die Werthe $1, 2 \ldots (p-1)$ durchläuft. Da ferner

$$\left(\frac{hs}{p}\right) = \left(\frac{h}{p}\right)\left(\frac{s}{p}\right), \quad \left(\frac{h}{p}\right)\left(\frac{h}{p}\right) = 1$$

ist, so wird

$$\varphi(h, p) = \left(\frac{h}{p}\right) \Sigma \left(\frac{hs}{p}\right) e^{hs.\frac{2\pi i}{p}},$$

---

*) *Disquisitiones Arithmeticae* art. 356.

**) *Summatio quarumdam serierum singularium* 1808.

oder, da h nicht theilbar durch p ist, und folglich hs gleichzeitig mit s ein vollständiges Restsystem nach dem Modul p durchläuft (mit Ausschluss der Zahl $\equiv 0$),

$$\varphi(h, p) = \left(\frac{h}{p}\right) \Sigma \left(\frac{s}{p}\right) e^{s\frac{2\pi i}{p}};$$

für $h = 1$ ergiebt sich

$$\varphi(1, p) = \Sigma \left(\frac{s}{p}\right) e^{s\frac{2\pi i}{p}}$$

und folglich (nach §. 114)

$$\varphi(h, p) = \left(\frac{h}{p}\right) \varphi(1, p) = \left(\frac{h}{p}\right) i^{\left(\frac{p-1}{2}\right)^2} \sqrt{p},$$

wo die Quadratwurzel $\sqrt{p}$ wieder positiv zu nehmen ist. (Wenn h durch p theilbar ist, so ergiebt sich unmittelbar aus der Definition dieser Summen $\varphi(h, p) = p$).

Aus dem vorstehenden Resultate in Verbindung mit dem dritten Satze des §. 113 lässt sich nun auf ganz einfache Weise das Reciprocitätsgesetz in der Theorie der quadratischen Reste (§. 42) für je zwei positive ungerade Primzahlen p und q ableiten. Es ist nämlich

$$\varphi(q, p) = \left(\frac{q}{p}\right) i^{1/4(p-1)^2} \sqrt{p}$$

und ebenso

$$\varphi(p, q) = \left(\frac{p}{q}\right) i^{1/4(q-1)^2} \sqrt{q}$$

und nach dem vorhergehenden Paragraphen

$$\varphi(1, pq) = i^{1/4(pq-1)^2} \sqrt{pq},$$

und zwar sind alle Quadratwurzeln *positiv* zu nehmen, woraus folgt, dass

$$\sqrt{pq} = \sqrt{p}\,\sqrt{q}$$

ist. Nach dem dritten Satze des §. 113 ist nun

$$\varphi(p, q)\,\varphi(q, p) = \varphi(1, pq),$$

folglich

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) i^{1/4(p-1)^2 + 1/4(q-1)^2} \sqrt{p} \sqrt{q} = i^{1/4(pq-1)^2} \sqrt{pq}$$

und also

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = i^{\lambda},$$

wo zur Abkürzung λ für

$$\frac{(pq-1)^2 - (p-1)^2 - (q-1)^2}{4} = \frac{p-1}{2} \frac{q-1}{2} \left\{(p+1)(q+1) - 2\right\}$$

gesetzt ist; da nun

$$(p+1)(q+1) - 2 \equiv 2 \pmod{4}$$

ist, so erhalten wir

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = i^{1/2(p-1)(q-1)} = (-1)^{1/2(p-1) \cdot 1/2(q-1)},$$

womit der Reciprocitätssatz von Neuem bewiesen ist. Dieser Beweis rührt ebenfalls von *Gauss* her *).

Auf ganz ähnliche Art lassen sich die Sätze (§§. 40, 41) über die Zahlen -1 und 2 beweisen. Aus dem obigen Satze

$$\varphi(h, p) = \left(\frac{h}{p}\right) \varphi(1, p) = \left(\frac{h}{p}\right) i^{1/4(p-1)^2} \sqrt{p}$$

folgt nämlich

$$\varphi(-1, p) = \left(\frac{-1}{p}\right) i^{1/4(p-1)^2} \sqrt{p};$$

andererseits ist

$$\varphi(-1, p) = \sum e^{s^2 \frac{2\pi(-i)}{p}},$$

und hieraus folgt, dass $\varphi(-1, p)$ durch Vertauschung von i mit $-i$ aus $\varphi(1, p)$ hervorgeht, dass also

$$\varphi(-1, p) = (-i)^{1/4(p-1)^2} \sqrt{p}$$

ist; durch Vergleichung dieser beiden Ausdrücke, in denen $\sqrt{p}$ beide Male positiv zu nehmen ist, ergiebt sich aber

*) *Summatio quarumdam serierum singularium.*

$$\left(\frac{-1}{p}\right) = (-1)^{1/4(p-1)^2} = (-1)^{1/2(p-1)}.$$

Setzen wir ferner in dem dritten Satz des §. 113

$$h = 1,\ m = 8,\ n = p,$$

so erhalten wir

$$\varphi(8, p)\,\varphi(p, 8) = \varphi(1, 8p);$$

nun ist aber

$$\varphi(1, 8p) = (1 + i)\sqrt{8p} = 4\sqrt{p}\,.\,e^{1/4\pi i},$$

ferner

$$\varphi(p, 8) = 4e^{1/4 p\pi i},$$

ferner (nach dem zweiten Satz des §. 113)

$$\varphi(8, p) = \varphi(2\,.\,2^2, p) = \varphi(2, p),$$

d. h.

$$\varphi(8, p) = \left(\frac{2}{p}\right)\varphi(1, p) = \left(\frac{2}{p}\right) i^{1/4(p-1)^2}\sqrt{p};$$

setzen wir diese Werthe für $\varphi(8, p)$, $\varphi(p, 8)$ und $\varphi(1, 8p)$ in die vorangehende Gleichung ein, so erhalten wir

$$\left(\frac{2}{p}\right) i^{1/4(p-1)^2}\sqrt{p}\cdot 4e^{1/4 p\pi i} = 4\sqrt{p}\cdot e^{1/4\pi i},$$

und hieraus folgt leicht

$$\left(\frac{2}{p}\right) = (-1)^{1/8(p^2-1)}.$$

Auf diese Weise sind alle Hauptsätze der Theorie der quadratischen Reste von Neuem bewiesen.

§. 116.

Für den Fall, dass p eine ungerade Primzahl und h irgend eine durch p nicht theilbare ganze Zahl ist, haben wir im vorigen Paragraphen folgende Gleichung erhalten

$$\varphi(h, p) = \Sigma\left(\frac{s}{p}\right) e^{s\frac{2h\pi i}{p}};$$

setzen wir hierin für $\varphi(h, p)$ seinen Werth ein, so sehen wir, dass die so entstehende Gleichung

$$\left(\frac{h}{p}\right) i^{\frac{1}{4}(p-1)^2} \sqrt{p} = \Sigma \left(\frac{s}{p}\right) e^{s \frac{2h\pi i}{p}}$$

selbst für den vorher ausgeschlossenen Fall gilt, in welchem $h \equiv 0 \pmod{p}$ ist, vorausgesetzt dass wir dann

$$\left(\frac{h}{p}\right) = 0$$

setzen (§. 102); denn die rechte Seite wird

$$\Sigma \left(\frac{s}{p}\right) = 0,$$

weil die Anzahl der quadratischen Reste genau gleich ist der Anzahl der quadratischen Nichtreste. Wir wollen nun im Folgenden immer

$$\left(\frac{m}{P}\right) = 0$$

setzen, so oft m keine relative Primzahl zu P ist (vergl. §. 46 und §. 102); in Folge dieser Bestimmung können wir die obige Gleichung auch folgendermaassen schreiben

$$\Sigma \left(\frac{s}{p}\right) e^{s \frac{2h\pi i}{p}} = \left(\frac{h}{p}\right) i^{\frac{1}{4}(p-1)^2} \sqrt{p},$$

wo in der Summe linker Hand der Summationsbuchstabe s ein vollständiges Restsystem (mit oder ohne Ausschluss von $s \equiv 0$) in Bezug auf den Modulus p durchlaufen muss. Wir wollen nun zeigen, dass dieser Satz über ungerade positive Primzahlen p sich genau in derselben Fassung auch auf alle positiven ungeraden zusammengesetzten Zahlen P übertragen lässt, vorausgesetzt, dass P durch keine Quadratzahl (ausser 1) theilbar ist. Wir setzen also

$$P = p\, p'\, p'' \ \ldots$$

wo $p, p', p'' \ldots$ lauter positive ungerade und von einander verschiedene Primzahlen bedeuten, und führen der Bequemlichkeit halber folgende Bezeichnung ein:

$$\frac{P}{p} = Q,\ \frac{P}{p'} = Q',\ \frac{P}{p''} = Q'' \ \ldots$$

Schreiben wir nun für jede der Primzahlen $p, p', p'' \ldots$ die obige Gleichung auf:

$$\Sigma \left(\frac{s}{p}\right) e^{s\frac{2h\pi i}{p}} = \left(\frac{h}{p}\right) i^{1/4(p-1)^2} \sqrt{p}$$

$$\Sigma \left(\frac{s'}{p'}\right) e^{s'\frac{2h\pi i}{p'}} = \left(\frac{h}{p'}\right) i^{1/4(p'-1)^2} \sqrt{p'}$$

$$\Sigma \left(\frac{s''}{p''}\right) e^{s''\frac{2h\pi i}{p''}} = \left(\frac{h}{p''}\right) i^{1/4(p''-1)^2} \sqrt{p''}$$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

und setzen wir zur Abkürzung

$$sQ + s'Q' + s''Q'' + \cdots = m,$$

so ergiebt, da auch nach der neuen Erweiterung des Legendre'schen Symbols stets

$$\left(\frac{h}{p}\right)\left(\frac{h}{p'}\right)\left(\frac{h}{p''}\right)\cdots = \left(\frac{h}{P}\right)$$

ist, die Multiplication aller dieser Gleichungen folgendes Resultat

$$\Sigma \left(\frac{s}{p}\right)\left(\frac{s'}{p'}\right)\left(\frac{s''}{p''}\right) \ldots e^{m\frac{2h\pi i}{P}}$$

$$= \left(\frac{h}{P}\right) i^{1/4(p-1)^2 + 1/4(p'-1)^2 + 1/4(p''-1)^2 + \cdots} \sqrt{P},$$

wo $\sqrt{P}$ wieder positiv zu nehmen ist, und das Summenzeichen linker Hand sich auf alle $pp'p'' \ldots = P$ Combinationen aller Werthe von $s, s', s'' \ldots$ bezieht. Zunächst leuchtet nun ein, dass je zwei verschiedenen dieser Combinationen auch zwei nach dem Modulus P incongruente Werthe von m entsprechen; denn aus

$$sQ + s'Q' + s''Q'' + \ldots \equiv tQ + t'Q' + t''Q'' + \ldots \pmod{P}$$

würde, da $Q', Q'' \ldots$ sämmtlich $\equiv 0 \pmod{p}$ sind, folgen, dass

$$sQ \equiv tQ \pmod{p},$$

und, da Q relative Primzahl zu p ist, auch

$$s \equiv t \pmod{p}$$

wäre; ähnlich würde aus derselben Annahme gleichzeitig

$$s' \equiv t' \pmod{p'};\quad s'' \equiv t'' \pmod{p''} \quad \ldots$$

folgen, so dass also die beiden Combinationen $s, s', s'' \ldots$ und

$t, t', t'' \ldots$ identisch wären. In der That durchläuft also m ein vollständiges Restsystem in Bezug auf den Modulus P. Ferner ist nun

$$\left(\frac{m}{p}\right) = \left(\frac{sQ + s'Q' + s''Q'' + \ldots}{p}\right) = \left(\frac{sQ}{p}\right) = \left(\frac{s}{p}\right)\left(\frac{Q}{p}\right),$$

und ebenso

$$\left(\frac{m}{p'}\right) = \left(\frac{s'}{p'}\right)\left(\frac{Q'}{p'}\right), \quad \left(\frac{m}{p''}\right) = \left(\frac{s''}{p''}\right)\left(\frac{Q''}{p''}\right) \quad \ldots,$$

folglich auch, wenn man alle diese Gleichungen multiplicirt,

$$\left(\frac{m}{P}\right) = \left(\frac{s}{p}\right)\left(\frac{s'}{p'}\right)\left(\frac{s''}{p''}\right) \cdots \left(\frac{Q}{p}\right)\left(\frac{Q'}{p'}\right)\left(\frac{Q''}{p''}\right) \cdots$$

Multiplicirt man daher beide Seiten der obigen Gleichung mit

$$\left(\frac{Q}{p}\right)\left(\frac{Q'}{p'}\right)\left(\frac{Q''}{p''}\right) \quad \ldots,$$

so erhält man

$$\Sigma\left(\frac{m}{P}\right) e^{m\frac{2h\pi i}{P}} = \left(\frac{Q}{p}\right)\left(\frac{Q'}{p'}\right)\left(\frac{Q''}{p''}\right) \cdots \left(\frac{h}{P}\right) i^{\Sigma \frac{1}{4}(p-1)^2} \sqrt{P},$$

wo rechts zur Abkürzung

$$\left(\frac{p-1}{2}\right)^2 + \left(\frac{p'-1}{2}\right)^2 + \left(\frac{p''-1}{2}\right)^2 + \ldots = \Sigma\left(\frac{p-1}{2}\right)^2$$

gesetzt ist. Da nun ferner

$$\left(\frac{Q}{p}\right) = \left(\frac{p'}{p}\right)\left(\frac{p''}{p}\right) \quad \ldots$$
$$\left(\frac{Q'}{p'}\right) = \left(\frac{p}{p'}\right)\left(\frac{p''}{p'}\right) \quad \ldots$$
$$\left(\frac{Q''}{p''}\right) = \left(\frac{p}{p''}\right)\left(\frac{p'}{p''}\right) \quad \ldots$$
$$\ldots\ldots\ldots\ldots\ldots$$

ist, so erhält man durch Multiplication

$$\left(\frac{Q}{p}\right)\left(\frac{Q'}{p'}\right)\left(\frac{Q''}{p''}\right) \cdots = \Pi\left(\frac{p}{p'}\right)\left(\frac{p'}{p}\right),$$

wo das Productzeichen Π sich auf alle möglichen Paare von je

zwei verschiedenen Primzahlen p, p' bezieht. Da nun nach dem Reciprocitätssatze

$$\left(\frac{p}{p'}\right)\left(\frac{p'}{p}\right) = (-1)^{\frac{1}{2}(p-1)\cdot\frac{1}{2}(p'-1)} = i^{\frac{1}{2}(p-1)(p'-1)}$$

ist, so erhält man

$$\left(\frac{Q}{p}\right)\left(\frac{Q'}{p'}\right)\left(\frac{Q''}{p''}\right)\cdots = i^{2\,\Sigma\,\frac{1}{2}(p-1)\cdot\frac{1}{2}(p'-1)},$$

wo das Summenzeichen rechter Hand sich wieder auf alle Combinationen von je zwei verschiedenen Primzahlen p, p' bezieht; es ist ferner

$$\Sigma\left(\frac{p-1}{2}\right)^2 + 2\,\Sigma\,\frac{p-1}{2}\,\frac{p'-1}{2} =$$
$$\left(\frac{p-1}{2} + \frac{p'-1}{2} + \frac{p''-1}{2} + \cdots\right)^2,$$

folglich

$$\Sigma\left(\frac{m}{P}\right) e^{m\frac{2h\pi i}{P}} = \left(\frac{h}{P}\right) i^{\left[\frac{1}{2}(p-1) + \frac{1}{2}(p'-1) + \cdots\right]^2} \sqrt{P}.$$

Da endlich (vergl. §. 46)

$$P = \Big(1 + (p-1)\Big)\Big(1 + (p'-1)\Big)\Big(1 + (p''-1)\Big)\cdots$$
$$\equiv 1 + (p-1) + (p'-1) + (p''-1) + \cdots \pmod{4}$$

und folglich

$$\frac{P-1}{2} \equiv \frac{p-1}{2} + \frac{p'-1}{2} + \frac{p''-1}{2} + \cdots \pmod{2}$$

und hieraus

$$\left(\frac{P-1}{2}\right)^2 \equiv \left(\frac{p-1}{2} + \frac{p'-1}{2} + \frac{p''-1}{2} \cdots\right)^2 \pmod{4}$$

ist, so ergiebt sich schliesslich

$$\Sigma\left(\frac{m}{P}\right) e^{m\frac{2h\pi i}{P}} = \left(\frac{h}{P}\right) i^{\frac{1}{4}(P-1)^2} \sqrt{P},$$

worin der zu beweisende Satz besteht. Ein specieller Fall, welcher oft zur Anwendung kommt und auch leicht auf andere Art zu beweisen ist (vergl. §. 52, I.), ergiebt sich durch die Annahme $h \equiv 0 \pmod{P}$; man erhält dann

$$\Sigma\left(\frac{m}{P}\right) = 0;$$

d. h. ist P eine positive ungerade Zahl, in welcher keine Quadratzahl (ausser 1) aufgeht, so ist die Anzahl aller derjenigen relativen Primzahlen m zu P, welche kleiner als P sind, und für welche $\left(\frac{m}{P}\right) = +1$ ist, genau gleich der Anzahl derjenigen Zahlen m, für welche $\left(\frac{m}{P}\right) = -1$ ist.

II. Ueber den Grenzwerth einer unendlichen Reihe.

§. 117.

Lehrsatz: Sind a und b zwei positive Constanten, so convergirt die unendliche Reihe

$$S = \frac{1}{b^{1+\varrho}} + \frac{1}{(b+a)^{1+\varrho}} + \frac{1}{(b+2a)^{1+\varrho}} + \frac{1}{(b+3a)^{1+\varrho}} + \cdots$$

für jeden positiven Werth von ϱ, *und bei unbegrenzter Abnahme dieser positiven Zahl* ϱ *nähert sich das Product* ϱS *dem Grenzwerthe* $\frac{1}{a}$.

Beweis. Construiren wir für einen bestimmten positiven Werth von ϱ die Curve, deren Gleichung in Bezug auf ein rechtwinkliges Coordinatensystem

$$y = \frac{1}{x^{1+\varrho}}$$

ist, so hat die Fläche, welche zwischen ihr und der unendlichen positiven Abscissenaxe liegt, von $x = b$ an gerechnet, den endlichen Werth

$$\int_b^{+\infty} y\,dx = \frac{1}{\varrho} \cdot \frac{1}{b^{\varrho}}.$$

Die Ordinaten der Curve, welche den Abscissen

$$b,\ b+a,\ b+2a,\ b+3a\ \ldots$$

entsprechen, sind

$$\frac{1}{b^{1+\varrho}},\ \frac{1}{(b+a)^{1+\varrho}},\ \frac{1}{(b+2a)^{1+\varrho}},\ \frac{1}{(b+3a)^{1+\varrho}}\ \cdots;$$

ihre Fusspuncte sind äquidistant und zerlegen die Abscissenaxe in unendlich viele Stücke von der Grösse a. Construirt man über jedem dieser Stücke als Grundlinie ein Rechteck, dessen Höhe gleich der letzten Ordinate in diesem Stück ist, so haben diese Rechtecke der Reihe nach den Flächeninhalt

$$\frac{a}{(b+a)^{1+\varrho}},\ \frac{a}{(b+2a)^{1+\varrho}},\ \frac{a}{(b+3a)^{1+\varrho}}\ \cdots$$

Da nun die Ordinate y der Curve mit stetig wachsendem x stetig abnimmt, so ist jedes dieser Rechtecke kleiner als der über demselben Abscissenstück liegende, bis zur Curve ausgedehnte Flächenstreifen, und folglich ist die Summe von noch so vielen jener Rechtecke stets kleiner als die gesammte, oben von der Curve begrenzte Fläche; d. h. es ist

$$\frac{a}{(b+a)^{1+\varrho}}+\frac{a}{(b+2a)^{1+\varrho}}+\frac{a}{(b+3a)^{1+\varrho}}+\cdots<\frac{1}{\varrho}\frac{1}{b^{\varrho}}$$

oder es ist, wenn auf beiden Seiten $\frac{a}{b^{1+\varrho}}$ addirt wird,

$$aS<\frac{1}{\varrho}\frac{1}{b^{\varrho}}+\frac{a}{b^{1+\varrho}},$$

woraus folgt, dass die aus lauter positiven Gliedern bestehende Reihe S wirklich für jeden positiven Werth von ϱ convergirt.

Construirt man nun über jedem der obigen Abscissenstücke als Grundlinie ein zweites Rechteck, dessen Höhe gleich der ersten Ordinate in diesem Stück ist, so sind diese Rechtecke, deren Flächeninhalt gleich

$$\frac{a}{b^{1+\varrho}},\ \frac{a}{(b+a)^{1+\varrho}},\ \frac{1}{(b+2a)^{1+\varrho}}\ \cdots,$$

nothwendig grösser als die über denselben Stücken liegenden, bis zur Curve fortgesetzten Flächenstreifen, aus dem schon oben angeführten Grunde, weil mit wachsendem x die Ordinate y stetig abnimmt. Die Summe aller dieser Rechtecke ist daher grösser als die gesammte, oben von der Curve begrenzte Fläche, d. h. es ist

$$aS>\frac{1}{\varrho}\frac{1}{b^{\varrho}}.$$

Auf diese Weise ist der Werth der unendlichen Reihe S und folglich auch der des Productes ϱS in zwei Grenzen eingeschlossen; es ist nämlich

$$\frac{1}{a}\,\frac{1}{b^{\varrho}} < \varrho S < \frac{1}{a}\,\frac{1}{b^{\varrho}} + \frac{\varrho}{b^{1+\varrho}}.$$

Wenn nun der positive Werth ϱ unendlich klein wird, so nähert sich sowohl

$$\frac{1}{a}\,\frac{1}{b^{\varrho}}, \text{ als auch } \frac{1}{a}\,\frac{1}{b^{\varrho}} + \frac{\varrho}{b^{1+\varrho}}$$

einem und demselben Grenzwerth $\frac{1}{a}$; mithin muss auch das Product ϱS sich demselben Grenzwerth $\frac{1}{a}$ nähern, was zu beweisen war.

§. 118.

Der so eben bewiesene Satz bildet nur einen speciellen Fall des folgenden, welcher seiner zahlreichen Anwendungen wegen von der grössten Wichtigkeit ist:

Es sei K ein System von positiven Zahlwerthen k, und T diejenige unstetige Function von einer positiven stetigen Veränderlichen t, welche angiebt, wie viele der in K enthaltenen Zahlwerthe k den Werth t nicht übertreffen; wenn nun mit unendlich wachsendem t der Quotient $T : t$ sich einem bestimmten endlichen Grenzwerth α nähert, so convergirt die Reihe

$$S = \Sigma \frac{1}{k^{1+\varrho}}$$

für jeden positiven Werth von ϱ, und das Product ϱS nähert sich mit unendlich abnehmendem ϱ demselben Grenzwerth α.

Es wird gut sein, dem Beweise dieses allgemeinen Princips einige erläuternde Bemerkungen vorauszuschicken. Zufolge der Bedeutung von T entspricht jedem endlichen Werth von t auch

ein endlicher Werth von T; denn wären in K unendlich viele Zahlen k enthalten, welche den endlichen Werth t nicht übertreffen, so würde auch jedem grössern Werth von t eine unendliche Anzahl T entsprechen; es würde daher das Verhältniss $T:t$ fortwährend unendlich gross sein; dies widerspricht aber der Annahme, dass $T:t$ sich einem endlichen Grenzwerth α mit wachsendem t nähert. Es leuchtet ferner ein, dass die ganze Zahl T nur dann ihren Werth ändert, wenn t einen Werth erreicht, welcher einer oder mehreren einander gleichen in K enthaltenen Zahlen k gleich ist, und zwar wird T dann plötzlich um ebenso viele Einheiten zunehmen, als es Zahlen k giebt, welche diesem Werth t gleich sind.

In dem einfachsten Fall, wenn K nur aus einer endlichen Anzahl von Zahlwerthen k besteht, leuchtet die Richtigkeit des obigen Satzes unmittelbar ein; denn sobald t dem grössten dieser Werthe k gleich geworden ist, bleibt T bei weiter wachsendem t unverändert; es ist folglich $\alpha = 0$; und da andererseits die Summe

$$\Sigma \frac{1}{k}$$

einen endlichen Werth hat, so wird auch das Product ϱS mit unendlich kleinem ϱ ebenfalls unendlich klein werden.

Ebenso bestätigt sich der allgemeine Satz in dem speciellen Fall, welcher in dem vorigen Paragraphen behandelt ist. Das System K besteht dort aus den sämmtlichen Zahlen von der Form $b + na$, die den sämmtlichen Werthen $0, 1, 2, 3 \ldots$ von n entsprechen; wenn nun $t = b + na$ oder $> b + na$, aber $< b + (n+1)\,a$ ist, so ist entsprechend $T = n + 1$, und folglich nähert sich der Quotient $T:t$ mit unendlich wachsendem t, also auch mit unendlich wachsendem n dem Grenzwerth

$$\alpha = \frac{1}{a};$$

und in der That haben wir gefunden, dass dieser Werth auch zugleich der Grenzwerth des Productes ϱS ist, wenn die positive Grösse ϱ unendlich klein wird.

§. 119.

Wir gehen nun zu dem Beweise des allgemeinen Satzes über und beginnen damit, die in K enthaltenen Zahlwerthe k ihrer Grösse nach zu ordnen und mit Indices zu versehen, in der Weise, dass

$$k_1 \leqq k_2 \leqq k_3 \leqq k_4 \leqq k_5 \ldots$$

wird; dies ist offenbar möglich, da unterhalb eines beliebigen endlichen positiven Werthes t immer nur eine endliche Anzahl von Zahlwerthen k vorhanden ist; sind mehrere Zahlen k gleich gross, so muss jede einzelne ihren besondern Index erhalten, so dass dann mehreren auf einander folgenden Indices gleich grosse Zahlwerthe k entsprechen.

Wir haben nun zu zeigen, erstens, dass die Reihe S für jeden positiven Werth von ϱ convergirt, zweitens, dass das Product ϱS mit unendlich abnehmendem positivem ϱ sich dem Grenzwerth α nähert; dies Letztere wird der Fall sein, wenn wir beweisen können, dass, wie klein auch eine gegebene positive Grösse δ sein mag, für hinreichend kleine Werthe von ϱ stets

$$\alpha - \delta < \varrho S < \alpha + \delta$$

wird. Schliessen wir für einen Augenblick den Fall, in welchem $\alpha = 0$ ist, von unserer Betrachtung aus, setzen wir also voraus, dass α ein positiver Werth ist (denn negativ kann α seiner Bedeutung nach nicht sein), so wählen wir, um diesen Nachweis zu liefern, beliebig nahe unterhalb und oberhalb α zwei positive Grössen β, γ von der Beschaffenheit, dass

$$\alpha - \delta < \beta < \alpha$$

und

$$\alpha + \delta > \gamma > \alpha$$

ist. Da nun der Quotient $T : t$ mit unendlich wachsendem t sich dem *zwischen* β und γ liegenden Werth α nähert, so wird immer ein endlicher positiver Werth τ existiren von der Beschaffenheit, dass für alle Werthe von t, welche $> \tau$ sind, stets

$$\beta \leqq \frac{T}{t} \leqq \gamma$$

ist. Es sei μ derjenige Werth von T, welcher dem Werthe $t = \tau$ entspricht, d. h. es seien

$$k_1, k_2, k_3, k_4 \dots k_{\mu-1}, k_\mu$$

sämmtliche in K enthaltenen Zahlwerthe k, welche diesen Werth τ nicht übertreffen; dann wollen wir zur Abkürzung

$$\frac{1}{k_1^{1+\varrho}} + \frac{1}{k_2^{1+\varrho}} + \frac{1}{k_3^{1+\varrho}} + \cdots + \frac{1}{k_\mu^{1+\varrho}} = S'$$

setzen.

Ist nun n irgend eine positive ganze Zahl, und zwar $n > \mu$, so ist $k_n > \tau$; es kann aber sein, dass mehrere in K enthaltene Zahlwerthe $= k_n$ sind; wir bezeichnen sie der Reihe nach mit $k_{m+1}, k_{m+2} \dots k_{m'}$. Für alle Werthe von t *zwischen* k_m und k_{m+1}, oder doch wenigstens für diejenigen dieser Werthe, welche zugleich $> \tau$ sind, ist nun $T = m$, also

$$\beta \leqq \frac{m}{t} \leqq \gamma;$$

wenn nun t dem Werth k_{m+1} unendlich nahe kommt, so wird

$$\lim \frac{m}{t} = \frac{m}{k_{m+1}} = \frac{m}{k_n},$$

woraus folgt, dass auch

$$\beta \leqq \frac{m}{k_n} \leqq \gamma$$

ist. Ferner entspricht dem Werth $t = k_{m+1} = k_n = k_{m'}$ der Werth $T = m'$, und es ist folglich auch

$$\beta \leqq \frac{m'}{k_n} \leqq \gamma;$$

hieraus folgt, da $n > m$ und ausserdem $n \leqq m'$ ist, dass auch

$$\beta \leqq \frac{n}{k_n} \leqq \gamma$$

ist; und dies gilt also für alle positiven ganzen Zahlen n, welche $> \mu$ sind. Für alle diese Zahlen ist daher

$$\beta^{1+\varrho} \frac{1}{n^{1+\varrho}} \leqq \frac{1}{k_n^{1+\varrho}} \leqq \gamma^{1+\varrho} \frac{1}{n^{1+\varrho}}, \qquad \text{(I)}$$

sobald $1+\varrho$ ein positiver Exponent ist, also gewiss, sobald ϱ selbst positiv ist, was wir in der Folge annehmen. Da nun nach dem in §. 117 behandelten speciellen Fall die unendliche Reihe

$$N = \frac{1}{(\mu+1)^{1+\varrho}} + \frac{1}{(\mu+2)^{1+\varrho}} + \frac{1}{(\mu+3)^{1+\varrho}} + \cdots$$

für jeden positiven Werth von ϱ convergirt, so gilt auch dasselbe von der unendlichen Reihe

$$S'' = \frac{1}{k^{1+\varrho}_{\mu+1}} + \frac{1}{k^{1+\varrho}_{\mu+2}} + \frac{1}{k^{1+\varrho}_{\mu+3}} + \cdots;$$

denn zufolge der Gleichung (I) ist die Summe von beliebig vielen Gliedern dieser Reihe S'' nicht grösser als das Product aus $\gamma^{1+\varrho}$ und der Summe der entsprechenden Glieder der Reihe N. Da ferner S' immer einen endlichen Werth hat, so *convergirt* auch die unendliche Reihe

$$S = \Sigma \frac{1}{k^{1+\varrho}} = S' + S''$$

für jeden positiven Werth von ϱ; hiermit ist der erste Theil unseres Satzes bewiesen.

Setzen wir nun in der Gleichung (I) für n alle ganzen Zahlen $\mu+1$, $\mu+2$, $\mu+3$ . . . ein, und addiren wir, so ergiebt sich

$$\beta^{1+\varrho} \cdot N \leqq S'' \leqq \gamma^{1+\varrho} \cdot N,$$

oder, wenn wir S' addiren und mit ϱ multipliciren,

$$\varrho S' + \beta^{1+\varrho} \cdot \varrho N \leqq \varrho S \leqq \varrho S' + \gamma^{1+\varrho} \cdot \varrho N.$$

Da nun S' immer endlich bleibt, und das Product ϱS nach §. 117 mit unendlich abnehmendem ϱ sich dem Grenzwerth 1 nähert, so leuchtet ein, dass die beiden Ausdrücke linker und rechter Hand von ϱS sich resp. den Grenzwerthen β und γ nähern. Da nun ferner $\beta > \alpha - \delta$, und $\gamma < \alpha + \delta$ gewählt war, so wird für hinreichend kleine Werthe von ϱ der Ausdruck linker Hand ebenfalls $> \alpha - \delta$, und der Ausdruck rechter Hand ebenfalls $< \alpha + \delta$ werden; und da der Werth von ϱS immer zwischen den Werthen dieser beiden Ausdrücke liegt, so wird für hinreichend kleine Werthe von ϱ wirklich

$$\alpha - \delta < \varrho S < \alpha + \delta$$

werden; hiermit ist nun auch der zweite Theil des Satzes bewiesen.

Für den oben ausgeschlossenen Fall $\alpha = 0$ gestaltet sich der Beweis noch einfacher; dann genügt nämlich der Nachweis, dass für hinreichend kleine Werthe von ϱ das Product $\varrho S < \delta$ wird; es genügt also die Einführung der einen Grösse γ*).

---

*) Es verdient bemerkt zu werden, dass man diesen Satz nicht umkehren darf. Besteht z. B. das System K aus einer Zahl $k = 1$, aus $(\Theta - 1)$ Zahlen $k = \Theta$, aus $(\Theta^2 - \Theta)$ Zahlen $k = \Theta^2$, aus $(\Theta^3 - \Theta^2)$ Zahlen $k = \Theta^3$ u. s. f., wo Θ eine positive ganze Zahl > 1 bedeutet, so ist für jeden positiven Werth von ϱ

$$S = 1 + \frac{\Theta - 1}{\Theta(\Theta^\varrho - 1)},$$

und das Product ϱS nähert sich mit unendlich abnehmendem ϱ dem Grenzwerthe

$$\alpha' = \frac{\Theta - 1}{\Theta \log \Theta},$$

während der Quotient $T : t$ bei unendlich wachsendem t fortwährend von dem Werth 1 abnehmend durch α' hindurch geht bis zu dem Werth $\frac{1}{\Theta}$, dann aber sogleich wieder zu dem Werth 1 zurückspringt, um von Neuem denselben Veränderungsprocess zu erleiden.

III. Ueber einen geometrischen Satz.

§. 120.

In einer Ebene sei eine vollständig begrenzte Figur F von allenthalben endlichen Dimensionen construirt, deren Flächeninhalt wir mit A bezeichnen wollen. Sind ferner X und Y zwei auf einander senkrechte Axen, und construirt man parallel mit ihnen zwei Systeme äquidistanter Parallelen, welche ein über die ganze Ebene ausgebreitetes Gitter bilden, so wird, wenn δ der Abstand je zweier benachbarter Parallelen, und T die Anzahl der Gitterpuncte ist, welche innerhalb F liegen, das Product $T\delta^2$ mit unendlich abnehmendem δ sich dem Grenzwerth A nähern.

Um diesen Satz zu beweisen, betrachten wir das System der mit Y parallelen Geraden und nehmen der Einfachheit halber an, dass jede derselben die Begrenzung der Figur nur zweimal schneidet; bezeichnen wir mit h die Länge des innerhalb F liegenden Stückes irgend einer solchen Parallelen, so ist $h\delta$ nahezu der Flächeninhalt des zwischen dieser und der folgenden Parallelen enthaltenen Theiles der Fläche F, und es wird in der Lehre von der Quadratur bewiesen, dass die Summe aller dieser Rechtecke $h\delta$ sich mit unendlich abnehmendem δ dem wahren Flächeninhalt A der Figur unbegrenzt nähert. Bezeichnen wir nun mit n die Anzahl der auf h liegenden Gitterpuncte (wobei es gleichgültig ist, ob ein zufällig auf der Begrenzung von F liegender Gitterpunct mitgezählt oder ausgeschlossen wird), so besteht h aus $(n-1)$ Stücken $= \delta$ und aus einem Rest, welcher höchstens $= 2\delta$ ist, so dass wir $h = n\delta + \varepsilon\delta$ setzen können, wo ε einen positiven oder negativen echten Bruch bedeutet. Es ist daher

$$\sum h\delta = \sum (n\delta^2 + \varepsilon\delta^2) = T\delta^2 + \delta \sum \varepsilon\delta;$$

es ist ferner, da ε absolut genommen höchstens $= 1$ ist, die Summe $\sum \varepsilon \delta$ höchstens gleich der endlichen Ausdehnung der Figur F in der Richtung der Axe X, und es wird daher $\delta \sum \varepsilon \delta$ mit δ gleichzeitig unendlich klein. Folglich nähert sich das Product $T\delta^2$ demselben Grenzwerthe A, welchem sich $\sum h \delta$ nähert; was zu beweisen war.

Es leuchtet übrigens ein, dass dieser Satz nicht an die Beschränkung gebunden ist, nach welcher die Parallelen mit der Axe Y nur einmal in die Figur F ein- und nur einmal aus ihr austreten. Man kann immer die Figur F als ein Aggregat von positiven und negativen Flächentheilen ansehen, welche einzeln der angegebenen Bedingung genügen; und wendet man auf jeden einzelnen Theil den Satz an, so ergiebt sich daraus sofort die Richtigkeit desselben für die ganze Figur F.

IV. Ueber die Genera, in welche die Classen der quadratischen Formen von bestimmter Determinante zerfallen*).

§. 121.

Ist (a, b, c) eine quadratische Form von der Determinante $b^2 - ac = D$, und sind z, z' irgend zwei durch diese Form darstellbare Zahlen (wobei es gleichgültig ist, ob die darstellenden Zahlen relative Primzahlen sind oder nicht), so lässt sich das Product zz' stets in die Form $x^2 - Dy^2$ bringen, wo x und y ganze Zahlen bedeuten; denn aus der Annahme

$$z = a\alpha^2 + 2b\alpha\gamma + c\gamma^2, \quad z' = a\beta^2 + 2b\beta\delta + c\delta^2$$

folgt (nach §. 54), dass die Form (a, b, c) durch die Substitution $\begin{pmatrix}\alpha, & \beta \\ \gamma, & \delta\end{pmatrix}$ in eine Form (z, x, z') übergeht, deren Determinante $x^2 - zz'$ von der Form Dy^2 ist. Aus dieser Bemerkung lassen sich folgende Schlüsse ziehen**).

1) Ist l eine ungerade in D aufgehende Primzahl, so hat für alle durch l nicht theilbaren Zahlen n, welche durch die Form (a, b, c) darstellbar sind, das Symbol

$$\left(\frac{n}{l}\right)$$

einen und denselben Werth. Denn sind n und n' irgend zwei solche durch l nicht theilbare und durch (a, b, c) darstellbare Zahlen, so folgt aus $nn' = x^2 - Dy^2$, dass $nn' \equiv x^2 \pmod{l}$, und folglich

*) *Dirichlet*: *Recherches sur diverses applications* etc. §§. 3, 6 (Crelle's Journal XIX).

**) Vergl. *Gauss*: *Disquiss. Arithmeticae* artt. 229—231.

$$\left(\frac{nn'}{l}\right) = +1, \text{ also } \left(\frac{n}{l}\right) = \left(\frac{n'}{l}\right)$$

ist.

2) Ist $D \equiv 3 \pmod{4}$, so hat für alle ungeraden durch die Form darstellbaren Zahlen n der Ausdruck

$$(-1)^{\frac{1}{2}(n-1)}$$

einen und denselben Werth. Denn sind n und n' irgend zwei solche ungerade Zahlen, so ist

$$nn' = x^2 - Dy^2 \equiv x^2 + y^2 \pmod{4};$$

da ferner nn' eine ungerade Zahl ist, so muss eine der beiden Zahlen x, y gerade, die andere ungerade sein; hieraus folgt $nn' \equiv 1 \pmod{4}$, also auch $n \equiv n' \pmod{4}$, und hieraus

$$(-1)^{\frac{1}{2}(n-1)} = (-1)^{\frac{1}{2}(n'-1)}.$$

3) Ist $D \equiv 2 \pmod{8}$, so hat für alle durch dieselbe Form darstellbaren ungeraden Zahlen n der Ausdruck

$$(-1)^{\frac{1}{8}(n^2-1)}$$

einen und denselben Werth. Denn aus

$$nn' = x^2 - Dy^2 \equiv x^2 - 2y^2 \pmod{8}$$

folgt, da x ungerade ist, $nn' \equiv \pm 1 \pmod{8}$, also auch $n \equiv \pm n'$ (mod. 8), woraus die obige Behauptung sich unmittelbar ergiebt.

4) Ist $D \equiv 6 \pmod{8}$, so hat für alle durch dieselbe Form darstellbaren ungeraden Zahlen n der Ausdruck

$$(-1)^{\frac{1}{2}(n-1)+\frac{1}{8}(n^2-1)}$$

einen und denselben Werth. Denn aus

$$nn' = x^2 - Dy^2 \equiv x^2 + 2y^2 \pmod{8}$$

folgt, da x ungerade ist, $nn' \equiv 1$ oder $\equiv 3 \pmod{8}$, je nachdem y gerade oder ungerade ist; dann ist entsprechend $n \equiv n'$ oder $\equiv 3n' \pmod{8}$, und man findet leicht, dass in beiden Fällen

$$\frac{n-1}{2} + \frac{n^2-1}{8} \equiv \frac{n'-1}{2} + \frac{n'^2-1}{8} \pmod{2}$$

ist, was zu beweisen war.

5) Ist $D \equiv 4 \pmod{8}$, so hat für alle durch dieselbe Form darstellbaren ungeraden Zahlen n der Ausdruck

$$(-1)^{\frac{1}{2}(n-1)}$$

einen und denselben Werth. Denn aus $nn' = x^2 - Dy^2$ folgt, da x ungerade ist, $nn' \equiv 1 \pmod{4}$, also $n \equiv n' \pmod{4}$.

6) Ist $D \equiv 0 \pmod{8}$, so hat für alle durch dieselbe Form darstellbaren ungeraden Zahlen n jeder der beiden Ausdrücke

$$(-1)^{\frac{1}{2}(n-1)} \text{ und } (-1)^{\frac{1}{8}(n^2-1)}$$

für sich einen unveränderlichen Werth. Denn aus

$$nn' = x^2 - Dy^2 \equiv x^2 \equiv 1 \pmod{8}$$

folgt $n \equiv n' \pmod{8}$.

§. 122.

Auf den Sätzen des vorigen Paragraphen beruht die Eintheilung der quadratischen Formen einer gegebenen Determinante D in *Genera*; wir beschränken uns hier auf die ursprünglichen Formen, weil das, was für sie gilt, leicht auf die andern Formen übertragen werden kann; ausserdem betrachten wir für den Fall einer negativen Determinante nur *positive*, d. h. solche Formen, deren äussere Coefficienten positiv sind. Es sei also (a, b, c) eine ursprüngliche Form der σten Art (§. 60), so wissen wir (§. 93), dass man den Variabeln derselben stets solche Werthe x, y beilegen kann, dass

$$\frac{ax^2 + 2bxy + cy^2}{\sigma} = n$$

positiv und relative Primzahl zu $2D$ wird; dabei ist es gleichgültig, ob x und y relative Primzahlen zu einander sind oder nicht. Bezeichnet man nun mit $l, l', l'' \ldots$ alle von einander verschiedenen in D aufgehenden ungeraden Primzahlen, so hat für alle durch eine und dieselbe Form (a, b, c) erzeugten Zahlen σn jedes der Symbole

$$\left(\frac{\sigma n}{l}\right), \left(\frac{\sigma n}{l'}\right), \left(\frac{\sigma n}{l''}\right) \ldots$$

und folglich auch jedes der Symbole

$$\left(\frac{n}{l}\right), \left(\frac{n}{l'}\right), \left(\frac{n}{l''}\right) \ldots$$

für sich einen unveränderlichen Werth; ist ferner D nicht $\equiv 1$

(mod. 4), also $\sigma = 1$, so gilt dasselbe, je nachdem $D \equiv 3$ (mod. 4), $D \equiv 2$ (mod. 8), $D \equiv 6$ (mod. 8), $D \equiv 4$ (mod. 8), $D \equiv 0$ (mod. 8) ist, entsprechend von dem Ausdruck

$$(-1)^{\frac{1}{2}(n-1)},\ (-1)^{\frac{1}{8}(n^2-1)},\ (-1)^{\frac{1}{2}(n-1)+\frac{1}{8}(n^2-1)},\ (-1)^{\frac{1}{2}(n-1)}$$

oder von jedem der beiden Ausdrücke

$$(-1)^{\frac{1}{2}(n-1)} \text{ und } (-1)^{\frac{1}{8}(n^2-1)}.$$

Die Anzahl dieser Ausdrücke

$$\left(\frac{n}{l}\right),\ \left(\frac{n}{l'}\right) \cdots (-1)^{\frac{1}{2}(n-1)} \text{ u. s. w.},$$

die wir die *Charaktere* C nennen wollen, hängt nur von der Determinante D ab und soll im Folgenden immer mit λ bezeichnet werden; offenbar ist λ gleich der Anzahl der in D aufgehenden ungeraden Primzahlen $l, l', l'' \ldots$, wenn $D \equiv 1$ (mod. 4); in den übrigen Fällen mit Ausnahme von $D \equiv 0$ (mod. 8) ist sie um 1, und im Fall $D \equiv 0$ (mod. 8) ist sie um 2 grösser. Das System der bestimmten Werthe ± 1, welche diesen λ Charakteren C für eine bestimmte Form (a, b, c) zukommen, wollen wir den *Total-Charakter* dieser Form nennen. Nach dem Ausfall dieses Total-Charakters theilen wir sämmtliche ursprüngliche Formen von gleicher Determinante und gleicher Art in *Genera* ein, indem wir je zwei Formen in dasselbe Genus oder in zwei verschiedene Genera werfen, je nachdem der Total-Charakter der einen Form mit dem der andern identisch ist, oder nicht; ein Genus ist hiernach der Inbegriff aller ursprünglichen Formen von gleicher Determinante und gleicher Art, für welche jeder der λ Charaktere C für sich genommen denselben Werth besitzt. Da nun alle Zahlen σn, welche durch eine bestimmte Form darstellbar sind, auch durch alle mit ihr äquivalenten Formen dargestellt werden können, so gehören alle Formen einer und derselben *Classe* auch in ein und dasselbe *Genus*; ein Genus ist daher immer der Inbegriff einer bestimmten Anzahl von Formen-Classen. Da ferner jeder der λ Charaktere C zwei einander entgegengesetzte Werthe haben kann, so leuchtet ein, dass die sämmtlichen ursprünglichen Formen von einer gegebenen Determinante D und von der σten Art *höchstens* 2^λ verschiedene Genera bilden können.

Wir bemerken nun noch, dass die äussern Coefficienten einer Form immer durch diese Form dargestellt werden, wenn man der einen Variabeln den Werth 1, der andern den Werth 0 beilegt;

mithin können die Charaktere dieser Form immer aus einem dieser beiden Coefficienten erkannt werden.

Beispiel 1: Für die Determinante $D = -35 \equiv 1 \pmod{4}$ bilden (§. 67) die sechs Formen

$$(1, 0, 35),\ (5, 0, 7),\ (3, \pm 1, 12), (4, \pm 1, 9)$$

ein vollständiges System nicht äquivalenter (positiver) Formen der ersten Art, und die beiden Formen

$$(2, 1, 18),\ (6, 1, 6)$$

ein solches Formensystem der zweiten Art. Um diese Formen (oder die durch sie repräsentirten Classen) in Genera einzutheilen, haben wir die beiden Charaktere

$$\left(\frac{n}{5}\right) \text{ und } \left(\frac{n}{7}\right)$$

zu betrachten, und da $\lambda = 2$ ist, so sind für jede der beiden Formenarten *höchstens vier* Genera zu erwarten. Die wirkliche Untersuchung ergiebt als Resultat folgende Tabelle:

(a, b, c)	$\left(\frac{n}{5}\right)$	$\left(\frac{n}{7}\right)$
(1, 0, 35)	+	+
(5, 0, 7)	—	—
(3, ±1, 12)	—	—
(4, ±1, 9)	+	+
(2, 1, 18)	+	+
(6, 1, 6)	—	—

Es zeigt sich also, dass jedes der beiden Systeme nur in *zwei* verschiedene Genera zerfällt; die drei Formen

$$(1, 0, 35),\ (4, \pm 1, 9)$$

bilden ein Genus, dessen Total-Charakter durch

$$\left(\frac{n}{5}\right) = +1,\ \left(\frac{n}{7}\right) = +1$$

bestimmt ist; die drei andern Formen

$$(5, 0, 7), \quad (3, \pm 1, 12)$$

bilden ein zweites Genus, dessen Total-Charakter durch

$$\left(\frac{n}{5}\right) = -1, \quad \left(\frac{n}{7}\right) = -1$$

bestimmt ist. Und jede der beiden Formen der zweiten Art bildet ein Genus für sich.

Beispiel 2: Für die Determinante $D = -5 \equiv 3 \pmod{4}$ bilden (§. 71) die beiden Formen

$$(1, 0, 5), \quad (2, 1, 3)$$

ein vollständiges System nicht äquivalenter (positiver) Formen; um sie in Genera einzutheilen, müssen wir die beiden Charaktere

$$(-1)^{\frac{1}{2}(n-1)} \text{ und } \left(\frac{n}{5}\right)$$

betrachten. Der Form (1, 0, 5) entspricht

$$(-1)^{\frac{1}{2}(n-1)} = +1, \quad \left(\frac{n}{5}\right) = +1,$$

und der Form (2, 1, 3) entspricht

$$(-1)^{\frac{1}{2}(n-1)} = -1, \quad \left(\frac{n}{5}\right) = -1.$$

Jede dieser beiden Formen bildet also ein Genus für sich; da $\lambda = 2$ ist, so ist auch hier die Anzahl der Genera nicht $= 2^{\lambda}$, sondern nur $= 2^{\lambda-1}$.

Beispiel 3: Für die Determinante $D = 24 \equiv 0 \pmod{8}$ findet man leicht (nach §§. 75, 78, 82), dass folgende vier Formen

$$(1, 4, -8), \quad (-1, 4, 8), \quad (3, 3, -5), \quad (-3, 3, 5)$$

ein vollständiges Formensystem bilden; es sind hier die folgenden drei Charaktere zu betrachten:

$$(-1)^{\frac{1}{2}(n-1)}, \quad (-1)^{\frac{1}{8}(n^2-1)}, \quad \left(\frac{n}{3}\right);$$

der ersten der obigen Formen entspricht

$$(-1)^{\frac{1}{2}(n-1)} = +1, \quad (-1)^{\frac{1}{8}(n^2-1)} = +1, \quad \left(\frac{n}{3}\right) = +1;$$

der zweiten

$$(-1)^{\frac{1}{2}(n-1)} = -1, \quad (-1)^{\frac{1}{8}(n^2-1)} = +1, \quad \left(\frac{n}{3}\right) = -1;$$

der dritten

$$(-1)^{\frac{1}{2}(n-1)} = -1, \quad (-1)^{\frac{1}{8}(n^2-1)} = -1, \quad \left(\frac{n}{3}\right) = +1;$$

und der vierten

$$(-1)^{\frac{1}{2}(n-1)} = +1, \quad (-1)^{\frac{1}{8}(n^2-1)} = -1, \quad \left(\frac{n}{3}\right) = -1.$$

Auch hier zeigt sich also, dass die Anzahl der wirklich vorhandenen Genera nicht $= 2^\lambda$, sondern nur $= 2^{\lambda-1}$ ist.

§. 123.

Mit Hülfe des Reciprocitätssatzes lässt sich nun in der That nachweisen, dass die Anzahl der verschiedenen Genera *höchstens* $= 2^{\lambda-1}$ ist. Wir setzen $D = D'S^2$, wo S^2 das grösste in D aufgehende Quadrat bezeichnet, und legen den Buchstaben δ, ε, P dieselbe Bedeutung in Bezug auf D' bei, welche sie in §. 101 in Bezug auf die dortige Determinante D erhalten haben. Dann wird

$$\left(\frac{D}{n}\right) = \left(\frac{D'}{n}\right) = \delta^{\frac{1}{2}(n-1)}\, \varepsilon^{\frac{1}{8}(n^2-1)} \left(\frac{n}{P}\right),$$

wo n jede beliebige positive ganze Zahl bedeutet, die relative Primzahl zu $2D$ ist. Da nun die Determinante D keine Quadratzahl, also D' nicht $= 1$ ist, so kann auch nicht gleichzeitig $\delta = +1$, $\varepsilon = +1$ und $P = 1$ sein, und hieraus folgt leicht, dass der Ausdruck

$$\delta^{\frac{1}{2}(n-1)}\, \varepsilon^{\frac{1}{8}(n^2-1)} \left(\frac{n}{P}\right)$$

entweder mit einem der Charaktere C, oder mit dem Producte aus mehreren dieser Charaktere identisch ist; bezeichnen wir diese Charaktere mit C' und ihr Product mit $\Pi C'$, so ist also stets

$$\Pi C' = \left(\frac{D}{n}\right),$$

sobald n positiv und relative Primzahl zu $2D$ ist. Da nun durch jede ursprüngliche Form der σten Art stets Zahlen σn dargestellt werden können, in welchen n dieser Bedingung genügt (§. 93), und zwar solche Zahlen σn, von welchen D quadratischer Rest ist

(§. 59), so ergiebt sich, dass der Total-Charakter einer jeden Form so beschaffen ist, dass stets

$$\Pi C' = +1$$

und niemals $\Pi C' = -1$ wird. Da nun unter den sämmtlichen 2^λ Zeichencombinationen, welche man erhält, wenn man jedem der λ Charaktere C sowohl den Werth $+1$ wie den Werth -1 beilegt, offenbar die Hälfte so beschaffen ist, dass $\Pi C' = -1$ wird, so folgt, dass diesen Zeichencombinationen oder Total-Charakteren keine wirklich existirenden Formen entsprechen können. Mithin ist die Anzahl der wirklich existirenden Genera höchstens $= 2^{\lambda-1}$.

Im Folgenden soll nun bewiesen werden, dass allen denjenigen Zeichencombinationen, welche in Uebereinstimmung mit der oben angegebenen Relation sind, wirklich existirende Formen entsprechen, dass also die Anzahl der wirklich vorhandenen Genera $= 2^{\lambda-1}$ ist, und ausserdem, dass jedes Genus eine gleiche Anzahl von Formen-Classen enthält.

§. 124.

Wir wollen wieder (wie in §. 89) mit n alle positiven ganzen Zahlen bezeichnen, die relative Primzahlen zu $2D$ sind, ferner mit m alle diejenigen Zahlen n, von welchen D quadratischer Rest ist, und mit μ die Anzahl der von einander verschiedenen in m aufgehenden Primzahlen. Es sei ferner $\psi(n)$ eine der Bedingung $\psi(n')\,\psi(n'') = \psi(n'\,n'')$ genügende Function, so ist stets

$$\Sigma\,\frac{\psi(n^2)}{n^{2s}} \times \Sigma\,\frac{2^\mu\,\psi(m)}{m^s} = \Sigma\,\frac{\psi(n)}{n^s} \times \Sigma\left(\frac{D}{n}\right)\frac{\psi(n)}{n^s},$$

vorausgesetzt, dass die hier vorkommenden unendlichen Reihen bestimmte von der Anordnung der Glieder unabhängige Werthe haben. Offenbar geht diese Gleichung durch die Specialisirung $\psi(n) = 1$ in die Endgleichung des §. 89 über, und sie könnte auch genau auf dieselbe Art wie diese bewiesen werden. Wir ziehen hier folgende Verification vor.

Verfährt man, wie in §. 91, so erhält man durch Ausführung der Multiplication der beiden unendlichen Reihen auf der rechten Seite

$$\Sigma\, \tau\, \frac{\psi(n)}{n^s}$$

wo

$$\tau = \Sigma \left(\frac{D}{\delta}\right)$$

ist, und δ alle Divisoren der Zahl n durchlaufen muss. Denkt man sich nun die Zahl n dargestellt als Product von Primzahlpotenzen $A, B \ldots$ und bezeichnet man mit a alle Divisoren von A, mit b alle Divisoren von B u. s. w., so leuchtet ein, dass τ das Product aus den Summen

$$\Sigma \left(\frac{D}{a}\right),\ \Sigma \left(\frac{D}{b}\right) \cdots$$

ist. Wenn nun z. B. $A = q^\alpha$, und q eine Primzahl ist, so wird

$$\Sigma \left(\frac{D}{a}\right) = \alpha + 1,$$

wenn D quadratischer Rest von q ist; ist dagegen D Nichtrest von q, so wird

$$\Sigma \left(\frac{D}{a}\right) = 1 \text{ oder } = 0,$$

je nachdem α gerade oder ungerade, d. h. je nachdem A ein Quadrat oder kein Quadrat ist. Bezeichnet man daher mit k alle diejenigen Zahlen n, in welchen nur solche Primfactoren aufgehen, von denen D Nichtrest ist, so folgt hieraus, dass jede Zahl n, für welche τ von Null verschieden ausfällt, von der Form mk^2 ist; und zwar ist dann τ gleich der Anzahl aller Divisoren von m. Da ferner $\psi(mk^2) = \psi(m)\,\psi(k^2)$ ist, so wird die rechte Seite unserer Gleichung gleich

$$\Sigma\, \frac{\tau\,\psi(mk^2)}{(mk^2)^s} = \Sigma\, \frac{\psi(k^2)}{k^{2s}} \cdot \Sigma\, \frac{\tau\,\psi(m)}{m^s}.$$

Wir wenden uns nun zur linken Seite; hier ist zunächst

$$\Sigma\, \frac{\psi(n^2)}{n^{2s}} = \Sigma\, \frac{\psi(k^2)}{k^{2s}}\, \Sigma\, \frac{\psi(m^2)}{m^{2s}},$$

und folglich braucht nur noch gezeigt zu werden, dass

$$\Sigma\, \frac{\psi(m^2)}{m^{2s}}\, \Sigma\, \frac{2^\mu\,\psi(m)}{m^s} = \Sigma\, \frac{\tau\,\psi(m)}{m^s}$$

ist. Führen wir links die Multiplication aus, indem wir alle Glieder des Productes, welche einen und denselben Nenner m^s haben, in ein einziges zusammenfassen, so erhalten wir ein Resultat von der Form

$$\sum \frac{\tau' \psi(m)}{m^s},$$

wo der Coefficient

$$\tau' = \sum 2^{\mu}$$

aus ebenso vielen Gliedern besteht, als die Zahl m quadratische Divisoren δ^2 besitzt, und wo die Zahl μ für jede Zerlegung von der Form $m = \varepsilon \delta^2$ angiebt, wie viele verschiedene Primzahlen in ε aufgehen. Es braucht daher jetzt nur noch nachgewiesen zu werden, dass $\tau' = \tau$ ist, d. h. es muss folgender Satz bewiesen werden:

Zerlegt man eine ganze positive Zahl m auf alle mögliche Arten in zwei Factoren, von denen der eine ein Quadrat δ^2 ist, und bezeichnet man mit μ jedesmal die Anzahl der in dem andern Factor ε aufgehenden von einander verschiedenen Primzahlen, so ist $\sum 2^{\mu}$ gleich der Anzahl τ aller Divisoren der Zahl m.

Von der Richtigkeit dieses Satzes überzeugt man sich aber leicht auf folgende Weise. Ist

$$m = a^{\alpha} b^{\beta} c^{\gamma} \ldots,$$

wo $a, b, c \ldots$ von einander verschiedene Primzahlen bedeuten, so ist jeder Divisor ε von der Form

$$\varepsilon = ABC \ldots,$$

wo $A, B, C \ldots$ resp. irgend welche Glieder aus den Reihen

$$\begin{array}{l} a^{\alpha},\; a^{\alpha-2},\; a^{\alpha-4} \ldots \\ b^{\beta},\; b^{\beta-2},\; b^{\beta-4} \ldots \\ c^{\gamma},\; c^{\gamma-2},\; c^{\gamma-4} \ldots \end{array}$$

u. s. w. bedeuten, welche so weit fortzusetzen sind, als die Exponenten nicht negativ werden. Lässt man nun jedem Factor $A, B, C \ldots$ resp. einen Factor $A', B', C' \ldots$ entsprechen, welcher $= 2$ oder $= 1$ ist, je nachdem der entsprechende Exponent > 0 oder $= 0$ ist, so wird

$$2^{\mu} = A' B' C' \ldots,$$

und folglich

$$\Sigma\, 2^{\mu} = \Sigma\, A' . \Sigma\, B' . \Sigma\, C' \ldots;$$

da aber, wie unmittelbar einleuchtet

$$\Sigma\, A' = \alpha + 1, \quad \Sigma\, B' = \beta + 1, \quad \Sigma\, C' = \gamma + 1 \ldots.$$

ist, so findet man

$$\Sigma\, 2^{\mu} = (\alpha + 1)\,(\beta + 1)\,(\gamma + 1) \ldots = \tau,$$

was zu beweisen war.

Die Richtigkeit der obigen Gleichung ist also hiermit ebenfalls erwiesen.

§. 125.

Nach §. 123 zerfallen die sämmtlichen positiven Formen von der Determinante D und von der σten Art, und also auch die sämmtlichen h Formenclassen in höchstens $\tau = 2^{\lambda-1}$ verschiedene Genera, deren Total-Charaktere sämmtlich der Bedingung

$$\Pi\, C' = +1$$

genügen, und die wir mit

$$G_1, G_2 \ldots G_\tau$$

bezeichnen wollen; die Anzahlen der Formen-Classen, welche diese Genera enthalten, sollen entsprechend mit

$$g_1, g_2 \ldots g_\tau$$

bezeichnet werden, so dass also, wenn eines dieser Genera, z. B. G_r, nicht wirklich vorhanden sein sollte, $g_r = 0$ zu setzen ist. Es soll nun gerade im Folgenden gezeigt werden, dass dies niemals eintritt, dass also diese τ Genera wirklich existiren, und ausserdem, dass sie alle gleich viele Formen-Classen enthalten, dass also

$$g_1 = g_2 = g_3 \cdots = \frac{1}{\tau}\, h$$

ist.

Zu diesem Zweck benutzen wir die im vorigen Paragraphen bewiesene Gleichung, und zwar verstehen wir unter $\psi(n)$ irgend

eins der $2^\lambda = 2\tau$ Glieder der Summe, welche durch die Entwickelung des über alle λ Charaktere C erstreckten Productes

$$\Pi\,(1 + C)$$

entsteht; der Bedingung $\psi(n)\,\psi(n') = \psi(nn')$ geschieht offenbar durch jede solche Specialisirung Genüge, denn alle Factoren C, aus denen ein solches $\psi(n)$ zusammengesetzt ist, genügen derselben Bedingung. Da ausserdem $\psi(n)$ für jede Zahl n, die relative Primzahl zu $2D$ ist, $= \pm 1$ ist, so convergiren die vier in der Gleichung vorkommenden unendlichen Reihen unabhängig von der Anordnung ihrer Glieder für jeden positiven Werth $s > 1$. Es ist also unter dieser Annahme

$$\Sigma \frac{1}{n^{2s}}\; \Sigma\, \psi(m)\, \frac{2^\mu}{m^s} = \Sigma\, \frac{\psi(n)}{n^s}\; \Sigma \left(\frac{D}{n}\right) \frac{\psi(n)}{n^s}.$$

Denken wir uns nun wieder (wie in §. 88) ein vollständiges System S von h Formen

$$(a, b, c),\;\; (a', b', c') \cdots$$

von der Determinante D und von der σten Art aufgeschrieben, und unterwerfen wir die Variabeln x, y jeder Form den dort angegebenen Bedingungen I), II), III), so wird jede Zahl σm im Ganzen auf $\varkappa\,.\,2^\mu$ verschiedene Arten erzeugt, wo $\varkappa$ die ebendaselbst festgesetzte, nur von D und σ abhängige Bedeutung hat. Die sämmtlichen h Formen des Systems S zerfallen nun in zwei Gruppen, nämlich in eine Gruppe von H Formen, die wir mit (a, b, c) bezeichnen wollen, für welche $\psi(m) = +1$ ist, und in eine zweite Gruppe von H' Formen, die wir mit (a', b', c') bezeichnen wollen, für welche $\psi(m) = -1$ ist. Offenbar werden auf diese Weise alle g_r Formen des Systems S, welche einem und demselben Genus G_r angehören, auch einer und derselben dieser beiden Gruppen zugetheilt; denn für alle diese Formen hat jeder Factor von $\psi(m)$ für sich genommen, und folglich auch $\psi(m)$ selbst einen und denselben Werth. Und umgekehrt leuchtet ein, dass alle Zahlen σm, denen $\psi(m) = +1$ entspricht, ausschliesslich durch Formen der ersten Gruppe, und alle Zahlen σm, denen $\psi(m) = -1$ entspricht, ausschliesslich durch Formen der zweiten Gruppe erzeugt werden.

Mithin ist

$$\varkappa\,\Sigma\,\psi(m)\,\frac{2^\mu}{m^s} = \left\{\begin{array}{l} +\,\Sigma\left(\dfrac{ax^2+2bxy+cy^2}{\sigma}\right)^{-s} + \cdots\cdot \\ -\,\Sigma\left(\dfrac{a'x^2+2b'xy+c'y^2}{\sigma}\right)^{-s} - \cdots\cdot \end{array}\right\},$$

wo auf der rechten Seite die den H Formen (a, b, c) der ersten Gruppe entsprechenden Doppelsummen mit positivem Vorzeichen, und die den H' Formen (a', b', c') der zweiten Gruppe entsprechenden Doppelsummen mit negativem Vorzeichen behaftet sind.

Multiplicirt man jetzt diese Gleichung mit der unendlichen Reihe

$$\Sigma\,\frac{1}{n^{2s}},$$

so erhält man links zufolge der obigen Gleichung das Resultat

$$\varkappa\,\Sigma\,\frac{\psi(n)}{n^s}\;\Sigma\left(\frac{D}{n}\right)\frac{\psi(n)}{n^s};$$

führt man ferner auf der rechten Seite die Multiplication wie in §. 90 aus, so verändert sich äusserlich ihre Gestalt nicht, sondern es fällt allein die frühere Bedingung III) fort, nach welcher die den Variabeln x, y beigelegten Werthe relative Primzahlen zu einander sein mussten. Man erhält daher

$$\varkappa\,\Sigma\,\frac{\psi(n)}{n^s}\,\Sigma\left(\frac{D}{n}\right)\frac{\psi(n)}{n^s} = \left\{\begin{array}{l} +\,\Sigma\left(\dfrac{ax^2+2bxy+cy^2}{\sigma}\right)^{-s} + \cdots\cdot \\ -\,\Sigma\left(\dfrac{a'x^2+2b'xy+c'y^2}{\sigma}\right)^{-s} - \cdots\cdot \end{array}\right\}.$$

Setzen wir jetzt $s = 1 + \varrho$, und multipliciren wir mit ϱ, so nähert sich mit unendlich abnehmendem positiven ϱ jedes der h Producte

$$\varrho\,\Sigma\left(\frac{ax^2+2bxy+cy^2}{\sigma}\right)^{-(1+\varrho)} \cdots \varrho\,\Sigma\left(\frac{a'x^2+2b'xy+c'y^2}{\sigma}\right)^{-(1+\varrho)} \cdots$$

einem und demselben von Null verschiedenen Grenzwerth W, welcher für eine negative Determinante in §. 95, für eine positive in §. 98 bestimmt ist; mithin wird der Grenzwerth, welchem sich das Product aus ϱ und aus der rechten Seite der vorstehenden Gleichung nähert, gleich $(H - H')\,W$.

Für die beiden Fälle nun, in welchen für $\psi(n)$ entweder das

Anfangsglied 1 oder das Glied $\Pi C'$ der Entwicklung des Productes $\Pi(1 + C)$ genommen wird, ist $H = h$ und $H' = 0$; und die obige Gleichung stimmt genau mit der in §. 90 überein, welche später zur Bestimmung der Classenanzahl h führte. In den übrigen $(2\tau - 2)$ Fällen, d. h. also, wenn unter $\psi(n)$ irgend ein Glied des entwickelten Ausdrucks

$$\Pi(1 + C) - 1 - \Pi C'$$

verstanden wird, nähert sich aber, wie im folgenden Paragraphen nachträglich gezeigt werden soll, jede der beiden unendlichen Reihen

$$\Sigma \frac{\psi(n)}{n^{1+\varrho}} \text{ und } \Sigma \left(\frac{D}{n}\right) \frac{\psi(n)}{n^{1+\varrho}}$$

mit unendlich abnehmendem ϱ einem *endlichen* Grenzwerth, und folglich das Product

$$\varrho\, k\, \Sigma \frac{\psi(n)}{n^{1+\varrho}} \cdot \Sigma \left(\frac{D}{n}\right) \frac{\psi(n)}{n^{1+\varrho}}$$

dem Grenzwerth Null. Vergleicht man dies mit dem oben gefundenen Grenzwerth $(H - H')\,W$, wo W eine von Null verschiedene Grösse war, so ergiebt sich

$$H - H' = 0,$$

d. h. jedem dieser $(2\tau - 2)$ Fälle entspricht eine Eintheilung aller h Formen des Systems S in zwei Gruppen, deren jede eine gleiche Anzahl $H = H' = \frac{1}{2} h$ Formen enthält.

Zufolge der obigen Bemerkung, dass die g_r Formen des Systems S, welche einem und demselben Genus G_r angehören, bei jeder einzelnen Specialisirung von $\psi(n)$ entweder alle in die erste, oder alle in die zweite Gruppe fallen, lässt sich jede solche Gleichung von der Form $H - H' = 0$, welche einem dieser $(2\tau - 2)$ Fälle entspricht, in folgender Weise aufschreiben

$$g_1 \pm g_2 \pm g_3 \pm \cdots \pm g_\tau = 0, \qquad (g)$$

wo die Anzahl g_1 jedesmal mit positivem, irgend eine andere Anzahl g_r aber mit positivem oder negativem Vorzeichen behaftet ist, je nachdem in diesem Fall die Formen des Genus G_r derselben Gruppe angehören, wie die Formen des Genus G_1, oder nicht, d. h. je nachdem die Werthe, welche $\psi(n)$ in dem Genus G_1 und

in dem Genus G_r erhält, gleich oder entgegengesetzt sind. Ist Δ der Ueberschuss der Anzahl der Fälle, in welchen das Erstere eintritt, über die Anzahl der übrigen, so wird, wenn man alle Gleichungen (g) addirt, die den $(2\tau - 2)$ verschiedenen Fällen entsprechen, der Coefficient von g_1 gleich $(2\tau - 2)$, und der von g_r gleich Δ werden. Um nun diesen Ueberschuss Δ zu bestimmen, bezeichnen wir mit γ_1 und γ_r die bestimmten Werthe ± 1, welche irgend einer der λ Charaktere C resp. in dem Genus G_1 und G_r annimmt, und unter diesen mit γ_1' und γ_r' diejenigen Werthe, welche den Charakteren C' entsprechen; man überzeugt sich dann leicht, dass

$$\Delta = \Pi\,(1 + \gamma_1\gamma_r) - 1 - \Pi\,\gamma_1'\gamma_r'$$

ist; denn wenn wir das erste, aus λ Factoren von der Form $(1 + \gamma_1\gamma_r)$ bestehende, Product rechter Hand entwickeln und die daraus entstehenden beiden Glieder 1 und $\Pi\,\gamma_1'\gamma_r'$ gegen die beiden andern Glieder fortheben, so bleiben $2^\lambda - 2 = 2\tau - 2$ Glieder zurück, deren jedes einem bestimmten Gliede des entwickelten Ausdrucks

$$\Pi\,(1 + C) - 1 - \Pi\,C',$$

d. h. einer bestimmten Specialisirung von $\psi(n)$ entspricht, und zwar wird ein solches Glied $= +1$ oder $= -1$ werden, je nachdem die beiden Werthe, welche das correspondirende $\psi(n)$ im Genus G_1 und im Genus G_r annimmt, gleich oder entgegengesetzt ausfallen; die algebraische Summe aller dieser Glieder ist also in der That gleich dem Ueberschuss Δ, was zu beweisen war. Da nun die beiden Genera G_1 und G_r verschieden sind, so ist mindestens einer der λ Factoren $(1 + \gamma_1\gamma_r)$ gleich Null, und da ausserdem $\Pi\,\gamma_1' = 1$, $\Pi\,\gamma_r' = 1$ und folglich auch $\Pi\,\gamma_1'\gamma_r' = 1$ ist, so erhalten wir $\Delta = -2$. Da dieser Ueberschuss Δ nun für alle von G_1 verschiedenen Genera gleich gross ist, so erhalten wir durch Addition sämmtlicher $(2\tau - 2)$ Gleichungen (g) das Resultat

$$(2\tau - 2)\,g_1 - 2\,(g_2 + g_3 + \cdots + g_\tau) = 0,$$

und da ausserdem

$$g_1 + g_2 + g_3 + \cdots + g_\tau = h$$

ist, so folgt

$$2\tau g_1 - 2h = 0, \text{ also } g_1 = \frac{h}{\tau} = \frac{h}{2^{\lambda-1}}.$$

Da endlich für jedes andere Genus $G_2, G_3 \cdots G_\tau$ die Untersuchung ebenso geführt werden kann, wie für das Genus G_1, so erhalten wir als Endresultat den Satz:

Die Anzahl der wirklich existirenden Genera ist gleich $2^{\lambda-1}$, *und alle diese Genera enthalten gleich viele Formenclassen*).*

§. 126.

Zur Vervollständigung des vorstehenden Beweises haben wir nun noch zu zeigen, dass für jede der $2\tau - 2$ Specialisirungen von $\psi(n)$, welche den Gliedern des obigen entwickelten Ausdrucks entsprechen, jede der beiden unendlichen Reihen

$$\Sigma \frac{\psi(n)}{n^{1+\varrho}}, \quad \Sigma \left(\frac{D}{n}\right) \frac{\psi(n)}{n^{1+\varrho}}$$

mit unendlich abnehmendem positiven ϱ sich einem endlichen Grenzwerth nähert. Dies kann mit Rücksicht auf frühere Untersuchungen (§. 101) in folgender Weise geschehen.

Jeder der beiden Coefficienten $\psi(n)$ und $\left(\frac{D}{n}\right)\psi(n)$ ist von der Form

$$\alpha_n = \theta^{1/2(n-1)} \eta^{1/8(n^2-1)} \left(\frac{n}{L}\right),$$

wo $\theta^2 = 1$, $\eta^2 = 1$, und L irgend ein ungerader Divisor von D ist; da quadratische Factoren im Nenner eines solchen Symbols $\left(\frac{n}{L}\right)$ fortgelassen werden dürfen, so können wir annehmen, dass L durch keine Quadratzahl (ausser 1) theilbar ist. Ferner ist jedenfalls nicht gleichzeitig $\theta = +1$, $\eta = +1$, $L = 1$; denn sonst wäre entweder $\psi(n) = 1$, oder $\psi(n) = \left(\frac{D}{n}\right) = \Pi C'$, gegen unsere Voraussetzung.

Bezeichnen wir mit LL' das Product aus allen von einander verschiedenen in D aufgehenden ungeraden Primzahlen, so ist das System der Zahlen n identisch mit dem System aller positiven ganzen Zahlen, welche relative Primzahlen zu $8LL'$ sind;

*) Vergl. *Disquisitiones Arithmeticae* artt. 252, 261, 287.

wir betrachten zunächst nur die ersten $\varphi(8\,L\,L')$ Zahlen n, d. h. diejenigen Zahlen n, welche kleiner als $8\,L\,L'$ sind, und zeigen, dass die Summe der entsprechenden Werthe von α_n gleich Null ist. Zu diesem Zweck bezeichnen wir mit a irgend eine der vier Zahlen 1, 3, 5, 7; mit b irgend eine der $\varphi(L)$ Zahlen, welche relative Primzahlen zu L und nicht grösser als L sind; endlich mit b' irgend eine der $\varphi(L')$ Zahlen, welche relative Primzahlen zu L' und nicht grösser als L' sind. Es wird dann (nach §. 25) durch die drei Congruenzen

$$n \equiv a \pmod{8},\ n \equiv b \pmod{L},\ n \equiv b' \pmod{L'}$$

eine und nur eine Zahl n bestimmt, welche relative Primzahl zu $8\,L\,L'$ und zugleich kleiner als $8\,L\,L'$ ist; und wenn jede der drei Zahlen a, b, b' unabhängig von den andern alle ihr zukommenden Werthe durchläuft, so werden auf diese Weise auch alle $\varphi(8\,L\,L')$ Zahlen n erzeugt, die relative Primzahlen zu $8\,L\,L'$ und kleiner als $8\,L\,L'$ sind. Da nun jedesmal

$$\theta^{\frac{1}{2}(n-1)}\ \eta^{\frac{1}{8}(n^2-1)} = \theta^{\frac{1}{2}(a-1)}\ \eta^{\frac{1}{8}(a^2-1)},\ \left(\frac{n}{L}\right) = \left(\frac{b}{L}\right)$$

ist, so wird die über diese Werthe von n ausgedehnte Summe

$$\Sigma\ \alpha_n = \varphi(L') \cdot \Sigma\ \theta^{\frac{1}{2}(a-1)}\ \eta^{\frac{1}{8}(a^2-1)} \cdot \Sigma \left(\frac{b}{L}\right);$$

nun ist aber (nach §. 52, I. oder nach §. 116)

$$\Sigma \left(\frac{b}{L}\right) = 0,$$

ausgenommen, wenn $L = 1$ ist; ausserdem findet man leicht, dass auch

$$\Sigma\ \theta^{\frac{1}{2}(a-1)}\ \eta^{\frac{1}{8}(a^2-1)} = 0$$

ist, ausgenommen, wenn gleichzeitig $\theta = +1$, $\eta = +1$ ist. Da nun in unserm Falle diese beiden Ausnahmefälle jedenfalls nicht gleichzeitig eintreten, so ist

$$\Sigma\ \alpha_n = 0,$$

wo das Summenzeichen sich auf die angegebenen Werthe von n bezieht.

Da ferner, sobald $n' \equiv n \pmod{8\,L\,L'}$, auch $\alpha_{n'} = \alpha_n$ ist, so wird immer

$$\Sigma\,\alpha_n = 0$$

sein, wenn die Summation auf beliebige $\varphi(8LL')$ auf einander folgende, also nach dem Modul $8LL'$ incongruente Werthe von n ausgedehnt wird. Und hieraus folgt unmittelbar, dass die Summe aller Werthe von α_n, die beliebig vielen auf einander folgenden Werthen von n entsprechen (von $n = 1$ an gerechnet) stets unterhalb einer endlichen angebbaren Grenze bleibt. Nach einer frühern Untersuchung (§. 101) ist daher die Reihe

$$\Sigma\,\frac{\alpha_n}{n^s},$$

wenn ihre Glieder nach der Grösse der Nenner geordnet werden, eine für jeden positiven Werth von s endliche und stetige Function von s; also nähert sich auch jede der beiden obigen Reihen mit unendlich abnehmendem positiven ϱ einem endlichen Grenzwerth, was zu beweisen war.

V. Theorie der Potenzreste für zusammengesetzte Moduli.

§. 127.

Es ist in §. 28 gezeigt, dass, wenn die Zahl a relative Primzahl gegen den Modul k ist, stets positive ganze Exponenten n von der Beschaffenheit existiren, dass $a^n \equiv 1 \pmod{k}$ ist; diese Exponenten n sind die sämmtlichen Vielfachen des kleinsten unter ihnen; bezeichnet man diesen mit δ, so sagt man, die Zahl a *gehöre* zum Exponenten δ; und die δ Zahlen

$$1,\ a,\ a^2 \ldots a^{\delta-1} \qquad (A)$$

sind sämmtlich incongruent. Mit Hülfe des verallgemeinerten Fermat'schen Satzes ist dort ebenfalls gezeigt, dass δ immer ein Divisor von $\varphi(k)$ ist; dies Resultat lässt sich aber auch ohne Hülfe des Fermat'schen Satzes ableiten durch eine eigenthümliche Methode, welche sehr häufig zum Nachweise der Theilbarkeit einer Zahl durch eine andere gebraucht werden kann. In unserm Falle gestaltet dieselbe sich folgendermaassen.

Ist a' irgend eine relative Primzahl zu k, so sind (nach §. 18) die δ Zahlen

$$a',\ a'a,\ a'a^2 \ldots a'a^{\delta-1} \qquad (A')$$

sämmtlich incongruent; dasselbe gilt von den δ Zahlen

$$a'',\ a''a,\ a''a^2 \ldots a''a^{\delta-1} \qquad (A'')$$

sobald a'' ebenfalls relative Primzahl zu k ist. Jeder solche Complex, wie A' oder A'', enthält δ unter einander incongruente Zahlen, die sämmtlich relative Primzahlen gegen k sind und also als Repräsentanten von δ Zahl-Classen in Bezug auf den Modul k angesehen werden können. Gesetzt nun, es findet sich eine und

dieselbe Zahlclasse in jedem der beiden Complexe A' und A'' vertreten, so giebt es zwei Exponenten μ', μ'' von der Beschaffenheit, dass

$$a' \cdot a^{\mu'} \equiv a'' \cdot a^{\mu''} \pmod{k}$$

ist; nehmen wir an, was der Symmetrie wegen erlaubt ist, dass $\mu'' \geqq \mu'$, so erhält man durch Division mit $a^{\mu'}$ die Congruenz

$$a' \equiv a'' \cdot a^{\mu'' - \mu'} \pmod{k};$$

und hieraus folgt sogleich, dass *jede* in A' enthaltene Zahl $a' \cdot a^m$ auch einer Zahl von der Form $a'' \cdot a^n$, d. h. einer in A'' enthaltenen Zahl congruent ist. Wir können hieraus schliessen, dass entweder zwei solche Complexe A', A'' dieselben δ Zahlclassen enthalten, oder dass keine einzige Classe in beiden gleichzeitig vertreten ist.

Bildet man nun der Reihe nach alle solche aus δ Zahlclassen bestehenden Complexe von der Form A', A'' . . ., und zwar nur solche, welche von einander verschieden sind, so muss endlich jede der $\varphi(k)$ Zahlclassen, welche relative Primzahlen zu k enthalten, in einem dieser Complexe, und auch nur in einem, vertreten sein; ist daher ε die Anzahl dieser von einander verschiedenen Complexe, so muss $\varphi(k) = \varepsilon\delta$, also $\varphi(k)$ theilbar durch δ sein, was zu beweisen war.

Hieraus ergiebt sich nun der Fermat'sche Satz als Folgerung; denn erhebt man die Congruenz

$$a^{\delta} \equiv 1 \pmod{k}$$

zur εten Potenz, so erhält man

$$a^{\varphi(k)} \equiv 1 \pmod{k}.$$

§. 128.

Für den Fall, dass der Modul k eine Primzahl p ist, wurde ferner in §. 29 bewiesen, dass zu jedem Divisor δ von $\varphi(p) = p - 1$ genau $\varphi(\delta)$ Zahlen gehören, die nach dem Modul p incongruent sind; und in §. 30 sind die Eigenschaften der sogenannten primitiven Wurzeln von p betrachtet, d. h. derjenigen $\varphi(p-1)$ incongruenten Zahlen g, welche zum Exponenten $p - 1$ selbst gehören.

Wir wollen nun untersuchen, ob ähnliche Gesetze auch für zusammengesetzte Moduln gelten.

Zunächst beschränken wir uns auf den Fall, in welchem der Modul k eine *Potenz von einer ungeraden Primzahl* p ist, und wir werden der Analogie nach unter einer *primitiven Wurzel* von k jede Zahl g verstehen, welche zum Exponenten $\varphi(k)$ gehört. Dem Beweise der wirklichen Existenz solcher primitiven Wurzeln schicken wir folgenden Hülfssatz voraus:

Ist h irgend eine ganze Zahl und $\pi \geqq 1$ eine positive ganze Zahl, so ist stets

$$(1 + hp^{\pi})^p \equiv 1 + hp^{\pi+1} \pmod{p^{\pi+2}}.$$

Man überzeugt sich hiervon leicht durch die Entwicklung der linken Seite nach dem binomischen Satze; man findet nämlich zunächst, indem man sich auf die drei ersten Glieder beschränkt,

$$(1 + hp^{\pi})^p \equiv 1 + hp^{\pi+1} + \tfrac{1}{2}(p-1)h^2p^{2\pi+1} \pmod{p^{3\pi}},$$

und hieraus ergiebt sich die obige Congruenz, wenn man bedenkt, dass p ungerade, also $\frac{1}{2}(p-1)$ eine ganze Zahl, und ferner, dass sowohl $p^{2\pi+1}$ als auch $p^{3\pi}$ durch $p^{\pi+2}$ theilbar ist.

Nach dieser Vorbemerkung gehen wir an unsere Untersuchung und nehmen zunächst einmal an, es existire für den Modul $p^{\pi+1}$, wo $\pi \geqq 1$ ist, wirklich eine primitive Wurzel g; dann liegt es nahe zu fragen: zu welchem Exponenten gehört eine solche Zahl g in Bezug auf den Modul p^{π}? Es sei δ dieser Exponent, also

$$g^{\delta} = 1 + hp^{\pi},$$

so erhält man mit Hülfe des soeben bewiesenen Satzes

$$g^{\delta p} \equiv 1 \pmod{p^{\pi+1}};$$

da nun g primitive Wurzel von $p^{\pi+1}$ ist, so muss δp durch $\varphi(p^{\pi+1}) = (p-1)p^{\pi}$, und folglich δ durch $(p-1)p^{\pi-1}$ theilbar sein; andererseits muss aber, da g zum Exponenten δ in Bezug auf den Modul p^{π} gehört, nothwendig $\varphi(p^{\pi}) = (p-1)p^{\pi-1}$ durch δ theilbar sein; mithin ist $\delta = \varphi(p^{\pi})$, d. h. g ist auch primitive Wurzel von p^{π}. Zugleich leuchtet ein, dass die in der Gleichung

$$g^{(p-1)p^{\pi-1}} = 1 + hp^{\pi}$$

vorkommende Zahl h nicht durch p theilbar sein kann; denn sonst wäre

$$g^{(p-1)p^{\pi-1}} \equiv 1 \pmod{p^{\pi+1}},$$

also g keine primitive Wurzel von $p^{\pi+1}$.

Setzt man diese Schlüsse weiter fort, so erhält man zunächst das Resultat:

Jede primitive Wurzel g von einer höhern Potenz einer ungeraden Primzahl p ist nothwendig eine primitive Wurzel der Zahl p selbst, und zwar von der Beschaffenheit, dass $g^{p-1}-1$ nicht durch p^2 theilbar ist.

Wir wollen nun umgekehrt annehmen, es sei g eine primitive Wurzel von p^π, und zwar von der Beschaffenheit, dass die in der Gleichung

$$g^{(p-1)p^{\pi-1}} = 1 + hp^\pi$$

vorkommende Zahl h nicht durch p theilbar ist; und wir fragen jetzt: zu welchem Exponenten gehört diese Zahl g in Bezug auf den Modul $p^{\pi+1}$? Ist δ dieser Exponent, also

$$g^\delta \equiv 1 \pmod{p^{\pi+1}},$$

so ist auch

$$g^\delta \equiv 1 \pmod{p^\pi},$$

und folglich δ theilbar durch $\varphi(p^\pi)$; da aber andererseits δ ein Divisor von $\varphi(p^{\pi+1}) = p\varphi(p^\pi)$ sein muss, so ist δ entweder $= \varphi(p^\pi)$, oder $= \varphi(p^{\pi+1})$; das Erstere ist aber nicht der Fall, weil unserer Voraussetzung zufolge die Zahl h nicht durch p theilbar ist; also ist $\delta = \varphi(p^{\pi+1})$, d. h. die Zahl g ist primitive Wurzel von $p^{\pi+1}$. Zugleich leuchtet aus der Congruenz

$$g^{(p-1)p^\pi} = (1 + hp^\pi)^p \equiv 1 + hp^{\pi+1} \pmod{p^{\pi+2}}$$

ein, dass die in der Gleichung

$$g^{(p-1)p^\pi} = 1 + h'p^{\pi+1}$$

vorkommende Zahl h' nicht durch p theilbar ist.

Durch Fortsetzung dieser Schlussweise erhalten wir das zweite Resultat:

Jede primitive Wurzel g einer ungeraden Primzahl p, für

welche die Differenz $g^{p-1}-1$ *nicht durch* p^2 *theilbar ist, ist auch eine primitive Wurzel aller höhern Potenzen von* p.

Um also die Existenz von primitiven Wurzeln g für höhere Potenzen von p nachzuweisen, und um alle diese Zahlen g zu finden, haben wir nur noch zu zeigen, dass in der That primitive Wurzeln g von p existiren, für welche $g^{p-1}-1$, oder, was dasselbe sagt, für welche g^p-g nicht durch p^2 theilbar ist. Dies geschieht leicht auf folgende Weise. Ist f eine primitive Wurzel von p, so sind alle in der Form

$$g = f + px$$

enthaltenen Zahlen g ebenfalls primitive Wurzeln von p; dann ist nach dem binomischen Satze

$$g^p \equiv f^p \pmod{p^2};$$

setzen wir daher

$$f^p \equiv f + f'p \pmod{p^2},$$

so wird

$$g^p - g \equiv p(f'-x) \pmod{p^2},$$

und folglich ist $g = f + px$ jedesmal eine primitive Wurzel aller Potenzen von p, ausgenommen, wenn $x \equiv f' \pmod{p}$, also

$$f + px \equiv f^p \pmod{p^2}$$

ist. Da nun $\varphi(p-1)$ nach dem Modul p incongruente Zahlen f existiren, und aus jeder Zahl f genau $(p-1)$ in Bezug auf den Modul p^2 incongruente Zahlen $g = f + px$ von der Beschaffenheit abgeleitet werden können, dass $g^{p-1}-1$ nicht durch p^2 theilbar wird, so erhalten wir das Resultat:

Die sämmtlichen primitiven Wurzeln von höhern Potenzen einer ungeraden Primzahl p *sind die sämmtlichen Individuen von* $(p-1)\,\varphi(p-1)$ *verschiedenen Zahlclassen in Bezug auf den Modul* p^2.

Beispiel: Sämmtliche primitive Wurzeln der Primzahl $p = 7$ sind in den beiden Reihen $7x+3$, $7x+5$ enthalten; da nun

$$3^7 \equiv 31, \quad 5^7 \equiv 19 \pmod{49}$$

ist, so sind alle in den arithmetischen Reihen $7x+3$, $7x+5$ enthaltenen Zahlen, mit Ausnahme derer, welche $\equiv 31$ oder $\equiv 19$ (mod. 49) sind, auch primitive Wurzeln von allen höhern Potenzen von 7.

§. 129.

Nachdem im Vorhergehenden die Existenz von primitiven Wurzeln g für jeden Modul p^π nachgewiesen ist, der eine Potenz einer ungeraden Primzahl p ist, kann man leicht die übrigen elementaren Fragen über die Potenzreste beantworten. Setzt man zur Abkürzung

$$\varphi(p^\pi) = c,$$

so sind die Potenzen

$$g^0,\ g^1,\ g^2 \ldots g^{c-1} \pmod{p^\pi}$$

sämmtlich incongruent, und bilden daher ein vollständiges System incongruenter Zahlen, mit Ausschluss der durch p theilbaren Zahlen. Ist daher n irgend eine durch p nicht theilbare Zahl, so existiren stets unendlich viele Exponenten γ, die aber nach dem Modul c sämmtlich einander congruent sind, von der Beschaffenheit, dass

$$n \equiv g^\gamma \pmod{p^\pi};$$

man nennt dann γ den *Index der Zahl n für die Basis g*, und drückt dies in Zeichen so aus

$$\text{Ind. } n \equiv \gamma \pmod{c};$$

durchläuft γ ein vollständiges Restsystem in Bezug auf den Modul c, so durchläuft n ein vollständiges System von Zahlen, die relative Primzahlen zu p^π und unter einander nach dem Modul p^π incongruent sind. Für die Rechnung mit diesen Indices gelten dieselben Gesetze, wie die (in §. 30 angegebenen) für den Fall $\pi = 1$. Wir heben hier besonders hervor, dass

$$\text{Ind. } (1) \equiv 0,\ \ \text{Ind. } (-1) \equiv \tfrac{1}{2} c \pmod{c},$$

und ferner, dass n quadratischer Rest oder Nichtrest von p^π ist, je nachdem Ind. n gerade oder ungerade ist.

Aus dem Index einer Zahl n lässt sich leicht der Exponent t bestimmen, zu welchem n in Bezug auf den Modul p^π gehört; aus

$$n \equiv g^{\text{Ind. } n} \pmod{p^\pi}$$

folgt nämlich

$$n^t \equiv g^{t \operatorname{Ind.} n} \pmod{p^\pi};$$

soll also $n^t \equiv 1$ sein, so muss t Ind. n durch c theilbar, und folglich t ein Multiplum von $\frac{c}{\delta}$ sein, wo δ den grössten gemeinschaftlichen Divisor von c und Ind. n bedeutet; die kleinste aller dieser Zahlen t, d. h. der Exponent, zu welchem n gehört, ist daher $= \frac{c}{\delta}$.

Hieraus folgt, dass n stets und nur dann eine primitive Wurzel von p^π ist, wenn Ind. n relative Primzahl zu c ist; die Anzahl aller nach dem Modul p^π incongruenten primitiven Wurzeln von p^π ist daher gleich der Anzahl derjenigen der Zahlen

$$0, \; 1, \; 2 \ldots c - 1,$$

welche relative Primzahlen zu c sind, also gleich $\varphi(c) = \varphi\varphi(p^\pi)$. Dasselbe Resultat ist aber auch eine unmittelbare Folge aus dem Schlusssatze des vorigen Paragraphen.

§. 130.

Die Primzahl 2 verhält sich anders als die ungeraden Primzahlen, welche bisher ausschliesslich betrachtet wurden.

Für den Modul 2 kann jede ungerade Zahl als primitive Wurzel angesehen werden.

Für den Modul $2^2 = 4$ ist $3 \equiv -1$ eine primitive Wurzel; zu jeder ungeraden Zahl n giebt es einen entsprechenden Exponenten α von der Beschaffenheit, dass

$$n \equiv (-1)^\alpha \pmod{4}$$

ist; und zwar ist $\alpha \equiv 0 \pmod{2}$, oder $\equiv 1 \pmod{2}$, je nachdem $n \equiv 1$ oder $\equiv 3 \pmod{4}$ ist.

Bis hierher findet also noch völlige Analogie mit den ungeraden Primzahlen Statt; sobald aber ein Modul 2^λ betrachtet wird, in welchem der Exponent $\lambda \geqq 3$ ist, hört dieselbe auf. Es lässt sich nämlich zeigen, dass, wenn n irgend eine ungerade Zahl bedeutet, immer schon

$$n^{\frac{1}{2}\varphi(2^\lambda)} = n^{2^{\lambda-2}} \equiv 1 \pmod{2^\lambda}$$

ist. In der That ist dieser Satz richtig für $\lambda = 3$; denn das Quadrat jeder ungeraden Zahl n ist $\equiv 1 \pmod{8}$. Nehmen wir

ferner an, der Satz sei für einen beliebigen Exponenten $\lambda \geqq 3$ schon bewiesen, es sei also

$$n^{2^{\lambda-2}} = 1 + h 2^{\lambda},$$

so folgt hieraus durch Quadriren

$$n^{2^{\lambda-1}} = 1 + h 2^{\lambda+1} + h^2 2^{2\lambda} \equiv 1 \pmod{2^{\lambda+1}},$$

d. h. der Satz gilt auch für den nächstfolgenden Exponenten $\lambda + 1$. Er gilt mithin allgemein, da er für $\lambda = 3$ gilt.

Es fragt sich nun, ob es in diesen Fällen wenigstens Zahlen giebt, die zu dem Exponenten $\frac{1}{2}\varphi(2^{\lambda}) = 2^{\lambda-2}$ gehören; man überzeugt sich leicht, dass die Zahl 5 diese Eigenschaft für jeden Modul $2^{\lambda} \geqq 8$ besitzt. Es ist nämlich

$$\begin{aligned} 5 &\equiv 1 + 4 \pmod{8} \\ 5^2 &\equiv 1 + 8 \pmod{16} \\ 5^4 &\equiv 1 + 16 \pmod{32} \\ 5^8 &\equiv 1 + 32 \pmod{64} \end{aligned}$$

allgemein

$$5^{2^{\lambda-3}} \equiv 1 + 2^{\lambda-1} \pmod{2^{\lambda}};$$

also

$$5^{2^{\lambda-3}} \text{ niemals } \equiv 1 \pmod{2^{\lambda}},$$

woraus unmittelbar folgt, dass der Exponent, zu welchem die Zahl 5 nach dem Modul 2^{λ} gehört, kein Divisor von $2^{\lambda-3}$ sein kann, und also, da er doch Divisor von $2^{\lambda-2}$ sein muss, nothwendig $= 2^{\lambda-2}$ ist.

Hieraus ergiebt sich nun, wenn man zur Abkürzung

$$\tfrac{1}{2}\varphi(2^{\lambda}) = 2^{\lambda-2} = b$$

setzt, dass die b Zahlen

$$5^0,\ 5^1,\ 5^2 \ldots 5^{b-1}$$

sämmtlich nach dem Modul 2^{λ} incongruent sind; dasselbe gilt von den Zahlen

$$-5^0,\ -5^1,\ -5^2 \ldots -5^{b-1}$$

da ferner die erstern sämmtlich $\equiv 1 \pmod{4}$, die letztern sämmtlich $\equiv 3 \pmod{4}$ sind; so bilden sie zusammengenommen ein System von $\varphi(2^{\lambda})$ nach dem Modul 2^{λ} incongruenten ungeraden

Zahlen. Ist daher n irgend eine ungerade Zahl, so kann man stets

$$n \equiv (-1)^{\alpha}\, 5^{\beta} \pmod{2^{\lambda}}$$

setzen, wo α nach dem Modul 2, und β nach dem Modul b vollständig bestimmt ist. Durchläuft α ein vollständiges Restsystem in Bezug auf den Modul 2, und β unabhängig von α ein vollständiges Restsystem in Bezug auf den Modul b, so durchläuft n ein vollständiges System von Zahlen, die in Bezug auf den Modul 2^{λ} incongruent und relative Primzahlen zu 2^{λ}, d. h. ungerade sind. Diese beiden Zahlen α und β kann man die *Indices* der Zahl n nennen; sie befolgen ganz ähnliche Gesetze, wie die Indices für die früher betrachteten Moduli. Wir heben noch besonders hervor, dass $n \equiv \pm 1$ oder $\equiv \pm 3 \pmod{8}$ ist, je nachdem β gerade oder ungerade.

Es verdient bemerkt zu werden, dass die vorstehende Form, in welche jede ungerade Zahl n gebracht werden kann, auch noch für den Fall $\lambda = 2$ gilt; die Anzahl b der Werthe von β reducirt sich nämlich auf 1, und da $5 \equiv 1 \pmod{4}$, so geht die obige Form in die frühere $n \equiv (-1)^{\alpha} \pmod{4}$ über. Für eine spätere Untersuchung ist es sogar zweckmässig, dieselbe Form der Darstellung aller relativen Primzahlen zu einem Modul von der Form 2^{λ} auf die Fälle $\lambda = 0$ und $\lambda = 1$ auszudehnen; da in denselben nur eine einzige Zahlclasse darzustellen ist, so wird man α und β auch nur einen einzigen Werth beizulegen haben; setzen wir daher $a = b = 1$, wenn $\lambda = 0$ oder $\lambda = 1$ ist, in allen andern Fällen ($\lambda \geqq 2$) aber $a = 2$, $b = \frac{1}{2}\varphi(2^{\lambda})$, so können wir sagen, dass der Ausdruck

$$n \equiv (-1)^{\alpha}\, 5^{\beta} \pmod{2^{\lambda}}$$

alle incongruenten relativen Primzahlen zum Modul durchläuft, wenn α und β resp. vollständige Restsysteme in Bezug auf a und b durchlaufen.

§. 131.

Es sei nun der Modul eine beliebige zusammengesetzte Zahl

$$k = 2^{\lambda}\, p^{\pi}\, p'^{\pi'} \ldots,$$

wo $p, p' \ldots$ von einander verschiedene ungerade Primzahlen, und

λ, π, π' ... ganze positive Exponenten bedeuten, deren erster, λ, auch $= 0$ sein kann. Ist n irgend eine relative Primzahl zu k, so kann man stets

$$n \equiv (-1)^{\alpha} 5^{\beta} \pmod{2^{\lambda}}$$
$$n \equiv g^{\gamma} \pmod{p^{\pi}}$$
$$n \equiv g'^{\gamma'} \pmod{p'^{\pi'}}$$
$$\cdots\cdots\cdots$$

setzen, wo g, g' ... primitive Wurzeln resp. von p^2, p'^2 ... bedeuten. Geben wir den Zahlen a, b die im vorigen Paragraphen festgesetzte Bedeutung, und setzen wir zur Abkürzung

$$\varphi(p^{\pi}) = c, \quad \varphi(p'^{\pi'}) = c' \ldots,$$

so sind die Exponenten oder Indices

$$\alpha, \ \beta, \ \gamma, \ \gamma' \ldots$$

vollständig bestimmt in Bezug auf die entsprechenden Moduli

$$a, \ b, \ c, \ c' \ldots,$$

und umgekehrt entspricht jedem solchen Systeme von Indices (nach §. 25) eine bestimmte Classe von Zahlen n nach dem Modul k, die relative Primzahlen zu k sind. Durchlaufen die Indices α, β, γ, γ' ... unabhängig von einander ihre a, b, c, c' ... Werthe, so durchläuft n sämmtliche

$$a b c c' \ldots = \varphi(k)$$

Zahlclassen in Bezug auf den Modul k, welche relative Primzahlen zu k enthalten.

Sind die Indices α, β, γ, γ' ... einer Zahl n bekannt, so ist es leicht, den Exponenten δ zu bestimmen, zu welchem die Zahl n gehört; denn offenbar ist δ das kleinste gemeinschaftliche Multiplum aller derjenigen Exponenten, zu welchen die Zahl n in Bezug auf die einzelnen Moduli 2^{λ}, p^{π}, $p'^{\pi'}$ ... gehört. Dieser Exponent δ ist daher immer ein Divisor von dem kleinsten gemeinschaftlichen Vielfachen μ der Zahlen a, b, c, c'... Es können daher primitive Wurzeln von k, d. h. Zahlen, die zum Exponenten $\varphi(k)$ gehören, nur dann existiren, wenn $\mu = \varphi(k)$ ist; man überzeugt sich leicht, dass dies nur dann der Fall ist, wenn der Modul $k = 1$, oder $= 2$, oder $= 4$, oder eine Potenz einer ungeraden

Primzahl, oder das Doppelte einer solchen Potenz ist; und umgekehrt leuchtet ein, dass in diesen Fällen immer primitive Wurzeln existiren.

Da ferner die Möglichkeit einer binomischen Congruenz von der Form

$$x^m \equiv n \pmod{k}$$

und die Anzahl ihrer Wurzeln nur von der Möglichkeit derselben Congruenz in Bezug auf die einzelnen Moduli 2^λ, p^π, $p'^{\pi'}$ ... abhängt (nach §. 37), so überzeugt man sich leicht, dass zur Beurtheilung dieser Frage und zur Auffindung der Wurzeln der Congruenz die Kenntniss der Indices der Zahl n vollständig ausreicht. Die wirkliche Ausführung dieser Untersuchung unterdrücken wir hier, weil sie sich ganz ebenso gestaltet wie in §. 31. Der Fall $m = 2$ würde auf diese Weise behandelt auf das in §. 37 gewonnene Resultat zurückführen. Ebenso leicht ist es, den verallgemeinerten Wilson'schen Satz (§. 38) von Neuem zu beweisen.

VI. Beweis des Satzes, dass jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Factor sind, unendlich viele Primzahlen enthält.

§. 132.

Der allgemeine Beweis dieses Satzes *) stützt sich auf die Betrachtung einer Classe von unendlichen Reihen von der Form

$$L = \Sigma\, \psi(n),$$

wo der Buchstabe n alle ganzen positiven Zahlen durchlaufen muss, und die reelle oder complexe Function $\psi(n)$ der Bedingung

$$\psi(n)\, \psi(n') = \psi(nn')$$

genügt. Hieraus folgt für $n = n' = 1$, dass $\psi(1) = 1$ oder $= 0$ ist; da aber im letztern Fall $\psi(n) = \psi(1)\, \psi(n)$ für alle Werthe von n verschwinden würde, so nehmen wir immer an, dass $\psi(1) = 1$ ist. Wir nehmen ferner an, die Function $\psi(n)$ sei so beschaffen, dass die Summe der analytischen Moduln aller Werthe $\psi(n)$ *endlich* ist, woraus folgt, dass die Reihe L einen von der Anordnung ihrer Glieder unabhängigen endlichen Werth besitzt. Man überzeugt sich dann leicht von der Richtigkeit der folgenden Gleichung

$$\Pi \frac{1}{1 - \psi(q)} = \Sigma\, \psi(n), \tag{I}$$

wo das Productzeichen sich auf alle, in beliebiger Ordnung auf einander folgenden, Primzahlen q bezieht.

---

*) Abhandlungen der Berliner Akademie aus dem Jahre 1837.

Zunächst leuchtet ein, da die Reihe L die Glieder

$$\psi(1) = 1,\ \psi(q) = z,\ \psi(q^2) = z^2 \ldots$$

enthält, und die Summe derselben für sich einen endlichen Werth hat, dass der Modulus von $\psi(q) < 1$, und folglich

$$\frac{1}{1 - \psi(q)} = 1 + \psi(q) + \psi(q^2) + \cdots$$

ist. Sind ferner $q_1, q_2, q_3 \ldots$ die sämmtlichen Primzahlen q, wie sie in dem Producte linker Hand aufeinander folgen, so wird das Product Q der ersten m Factoren

$$\frac{1}{1 - \psi(q_1)},\ \frac{1}{1 - \psi(q_2)} \cdots \frac{1}{1 - \psi(q_m)},$$

wenn man jeden derselben nach der vorstehenden Gleichung in eine unendliche Reihe entwickelt und die Multiplication ausführt, gleich $\Sigma\psi(l)$, wo die Summation über alle die ganzen positiven Zahlen l auszudehnen ist, in welchen keine andern als die Primzahlen $q_1, q_2 \ldots q_m$ aufgehen. Ist daher h irgend eine positive ganze Zahl, und nimmt man m so gross, dass unter den Primzahlen $q_1, q_2 \ldots q_m$ alle diejenigen enthalten sind, welche $< h$ sind, so enthält $\Sigma\psi(l)$ alle Glieder der Reihe $\Sigma\psi(n)$, in welchen $n < h$ ist, und ausserdem noch unendlich viele andere, in denen $n > h$ ist. Mithin unterscheidet sich das Product Q von der Summe $\Sigma\psi(n)$ um eine Summe von der Form $\Sigma\psi(n')$, in welche aber nur noch Zahlen n' eingehen, welche $\geqq h$ sind. Da nun die Summe der Moduln aller Glieder $\psi(n)$ endlich ist, so kann man h, und also auch m so gross wählen, dass die Summe der Moduln aller Glieder $\psi(n')$, und folglich auch der Modul der Differenz $Q - \Sigma\psi(n)$ kleiner wird als jede vorher gegebene Grösse; d. h. mit unbegrenzt wachsendem m nähert sich Q dem Grenzwerth $\Sigma\psi(n)$, was zu beweisen war.

Ausser diesen Reihen von der Form $L = \Sigma\psi(n)$ haben wir noch diejenigen Reihen zu betrachten, welche durch die Entwicklung ihrer natürlichen Logarithmen entstehen. Wenn der Modulus von z ein echter Bruch ist, so ist bekanntlich

$$z + \tfrac{1}{2}z^2 + \tfrac{1}{3}z^3 + \tfrac{1}{4}z^4 + \cdots = \log\frac{1}{1 - z},$$

und zwar ist der imaginäre Bestandtheil des Logarithmen rechter Hand stets zwischen den Grenzen $-\frac{1}{2}\pi i$ und $+\frac{1}{2}\pi i$ zu nehmen. Setzt man hierin $z = \psi(q)$ und für q alle Primzahlen, so erhält man zufolge der Gleichheit (I)

$$\Sigma\, \psi(q) + \tfrac{1}{2}\, \Sigma\, \psi(q^2) + \tfrac{1}{3}\, \Sigma\, \psi(q^3) + \cdots = \log L \qquad \text{(II)}$$

und offenbar hat die aus unendlich vielen unendlichen Reihen bestehende linke Seite einen von der Anordnung der Summationen unabhängigen endlichen Werth, weil selbst die Summe der Moduln aller ihrer Glieder einen endlichen Werth besitzt. Der imaginäre Theil des Logarithmen rechter Hand ist die Summe aller imaginären Theile der Logarithmen der einzelnen Factoren, aus denen das obige unendliche Product besteht.

Wir fügen zu diesem Resultat noch einige Bemerkungen hinzu. Ist zunächst $\psi(n)$ eine reelle Function, so sind alle Factoren des unendlichen Productes positiv, also ist $\log L$ reell, und da die Reihe $\log L$ einen endlichen Werth hat, so ist L ein positiver von Null verschiedener Werth. Ist aber $\psi(n)$ imaginär, und $\psi'(n)$ der jedesmal mit $\psi(n)$ conjugirte complexe Werth, so ist auch $\psi'(n)\, \psi'(n') = \psi'(nn')$, und die über alle ganzen positiven Zahlen n ausgedehnte Summe $L' = \Sigma\, \psi'(n)$ ist die mit $L = \Sigma\, \psi(n)$ conjugirte Zahl. Zugleich wird

$$\Sigma\, \psi'(q) + \tfrac{1}{2}\, \Sigma\, \psi'(q^2) + \tfrac{1}{3}\, \Sigma\, \psi'(q^3) + \cdots = \log L',$$

und zwar ist $\log L'$ conjugirt mit $\log L$, so dass die Summe $\log L + \log L' = \log(L L')$ reell wird.

Ist endlich der Werth der Function ψ für alle in einer bestimmten Zahl k aufgehenden Primzahlen $= 0$, so ist $\psi(n)$ jedesmal $= 0$, wenn n keine relative Primzahl zu k ist, und die Gleichungen (I) und (II) bleiben richtig, wenn man n alle relativen Primzahlen zu k, und q alle in k nicht aufgehenden Primzahlen durchlaufen lässt.

§. 133.

Es sei nun (wie in §. 131) k eine beliebige positive ganze Zahl, und zwar

$$k = 2^\lambda p^\pi p'^{\pi'} \ldots,$$

wo $p, p' \ldots$ von einander verschiedene ungerade Primzahlen bedeuten; wir geben ferner den Buchstaben

$$a,\ b,\ c,\ c' \ldots$$

ihre frühere Bedeutung (§. 131) und bezeichnen entsprechend mit

$$\theta,\ \eta,\ \omega,\ \omega' \ldots$$

irgend welche Wurzeln der Gleichungen

$$\theta^a = 1,\quad \eta^b = 1,\quad \omega^c = 1,\quad \omega'^{c'} = 1 \ldots$$

Ist nun n irgend eine positive ganze Zahl und zugleich relative Primzahl zu k, und sind ihre Indices

$$\alpha \,(\text{mod. } a),\quad \beta \,(\text{mod. } b),\quad \gamma \,(\text{mod. } c),\quad \gamma' \,(\text{mod. } c') \ldots,$$

so genügt, wie man leicht sieht, der Ausdruck

$$\psi(n) = \frac{\theta^\alpha \eta^\beta \omega^\gamma \omega'^{\gamma'} \ldots}{n^s}$$

der Bedingung $\psi(n)\,\psi(n') = \psi(nn')$; wenn ferner der Exponent $s > 1$ ist, was wir im Folgenden annehmen wollen, so ist die Summe der Moduln n^{-s} aller Glieder $\psi(n)$ endlich (§. 117), und folglich gelten die Gleichungen (I) und (II) des vorigen Paragraphen

$$\Pi \frac{1}{1 - \psi(q)} = \Sigma\, \psi(n) = L$$

$$\Sigma\, \psi(q) + \tfrac{1}{2}\, \Sigma\, \psi(q^2) + \tfrac{1}{3}\, \Sigma\, \psi(q^3) + \cdots = \log L$$

in welchen q alle in k nicht aufgehenden Primzahlen, n alle relativen Primzahlen zu k durchlaufen muss; beide Reihen haben, so lange $s > 1$ ist, bestimmte von der Anordnung ihrer Glieder unabhängige Summen. Wir können hinzufügen, dass beide Reihen auch *stetige* Functionen von s sind, so lange $s > 1$ ist; wir beweisen diese Behauptung für alle Werthe von s, welche grösser als ein beliebiger unechter Bruch σ sind, weil hieraus offenbar die Stetigkeit dieser Reihen für alle Werthe von $s > 1$ (excl. 1) folgt.

Denkt man sich jede der beiden Reihen L und $\log L$ in die Form $u + vi$ gebracht, so sind u und v von der Form

$$\frac{\alpha_1}{1^s} + \frac{\alpha_2}{2^s} + \frac{\alpha_3}{3^s} + \cdots,$$

wo die reellen Coefficienten α_1, α_2, α_3 ... ihrem absoluten Werth nach sämmtlich eine endliche Grösse A $(=1)$ nicht übertreffen. Um die Stetigkeit einer Function von s innerhalb eines gewissen Intervalls $(s \geqq \sigma)$ zu beweisen, genügt es darzuthun, dass, wie klein auch eine positive gegebene Grösse δ sein mag, die Function jedesmal in einen ersten und zwar stetigen, und in einen zweiten Bestandtheil zerlegt werden kann, der innerhalb des ganzen Intervalls $(s \geqq \sigma)$ dem absoluten Werth nach $< \delta$ ist; denn hieraus folgt, dass die Grösse einer plötzlichen Werthänderung der ganzen Function, die doch nur von dem zweiten Bestandtheil herrühren kann, kleiner als 2δ, und folglich, da die gegebene Grösse δ beliebig klein sein darf, nothwendig $= 0$ sein muss. In unserm Falle ergiebt sich die Möglichkeit einer solchen Zerlegung auf folgende Weise; ist n eine beliebige ganze Zahl, so ist die Summe der ersten n Glieder

$$\frac{\alpha_1}{1^s} + \frac{\alpha_2}{2^s} + \cdots + \frac{\alpha_n}{n^s}$$

eine stetige Function; die Summe aller folgenden Glieder ist ihrem absoluten Werth nach kleiner als

$$A\left(\frac{1}{(n+1)^s} + \frac{1}{(n+2)^s} + \cdots\right)$$

und folglich für alle Werthe $s \geqq \sigma$ auch kleiner als

$$A\left(\frac{1}{(n+1)^\sigma} + \frac{1}{(n+2)^\sigma} + \cdots\right);$$

da nun σ ein unechter Bruch ist, und folglich (nach §. 117) die Reihe

$$\frac{1}{1^\sigma} + \frac{1}{2^\sigma} + \frac{1}{3^\sigma} + \cdots$$

convergirt, so kann für jede gegebene Grösse δ entsprechend n so gross gewählt werden, dass

$$A\left(\frac{1}{(n+1)^\sigma} + \frac{1}{(n+2)^\sigma} + \cdots\right) < \delta$$

wird; hiermit ist für jede gegebene Grösse δ die Möglichkeit einer Zerlegung unserer Reihe in zwei Bestandtheile von der obigen Art, und also auch die Stetigkeit der Reihen L und $\log L$ für jeden Werth $s > 1$ nachgewiesen.

Der Beweis des Satzes über die arithmetische Progression gründet sich nun auf die Untersuchung des Verhaltens der Reihen L und $\log L$ bei unbegrenzter Annäherung des Exponenten s an den Werth 1. Wir bemerken zunächst, dass diese Reihen je nach der Wahl der in dem Ausdruck $\psi(n)$ vorkommenden Einheits-Wurzeln θ, η, ω, $\omega' \ldots$ ein ganz verschiedenes Verhalten zeigen; da diese Wurzeln resp. a, b, c, $c' \ldots$ verschiedene Werthe haben können, so sind in der Form L im Ganzen

$$a\,b\,c\,c' \ldots = \varphi(k)$$

verschiedene besondere Reihen enthalten; wir theilen diese Reihen L in drei Classen ein:

In die erste Classe nehmen wir nur eine einzige Reihe L_1 auf, und zwar diejenige, in welcher alle Einheits-Wurzeln θ, η, ω, $\omega' \ldots$ den Werth $+1$ haben.

In die zweite Classe nehmen wir alle übrigen Reihen L_2 auf, in welchen alle Einheits-Wurzeln reelle Werthe, also die Werthe ± 1 haben.

In die dritte Classe nehmen wir alle übrigen Reihen L_3 auf, d. h. alle diejenigen, in welchen wenigstens eine der Einheits-Wurzeln imaginär ist. Die Anzahl dieser Reihen ist jedenfalls gerade, und sie sind paarweise mit einander conjugirt; denn entspricht eine solche Reihe L_3 den Wurzeln θ, η, ω, $\omega' \ldots$, so entspricht immer eine zweite solche Reihe L'_3 den Wurzeln θ^{-1}, η^{-1}, ω^{-1}, $\omega'^{-1} \ldots$, und diese beiden Systeme von Wurzeln sind nicht identisch.

Wir wollen nun das Verhalten aller dieser Reihen genau untersuchen, wenn der Exponent $s = 1 + \varrho$ sich dem Werth 1 nähert, d. h. also, wenn die positive Grösse ϱ unendlich klein wird.

§. 134.

Betrachten wir zunächst das Verhalten der ersten Reihe

$$L_1 = \Sigma \frac{1}{n^s} = \Sigma \frac{1}{n^{1+\varrho}},$$

in welcher n alle relativen Primzahlen zu k durchlaufen muss, so

leuchtet ein, dass dieselbe als ein Aggregat von $\varphi(k)$ Partialreihen von der Form

$$\frac{1}{\nu^{1+\varrho}} + \frac{1}{(\nu + k)^{1+\varrho}} + \frac{1}{(\nu + 2k)^{1+\varrho}} + \cdots$$

angesehen werden kann, wo ν relative Primzahl zu k und $\leqq k$ ist. Da nun (nach §. 117) das Product aus einer solchen Reihe und aus ϱ mit unendlich abnehmendem ϱ sich einem endlichen positiven, von Null verschiedenen Grenzwerth nähert, so können wir

$$L_1 = \frac{l}{\varrho}$$

setzen, wo l mit unendlich abnehmendem ϱ sich ebenfalls einem endlichen, positiven, von Null verschiedenen Grenzwerth nähert.

Ganz anders verhalten sich aber die Reihen L der zweiten und dritten Classe; wir haben gesehen, dass alle diese Reihen, so lange $s > 1$ ist, bestimmte von der Anordnung ihrer Glieder unabhängige Werthe besitzen; von jetzt an wollen wir aber ihre Glieder $\psi(n)$ so anordnen, dass die Zahlen n ihrer Grösse nach wachsend auf einander folgen; die so geordneten Reihen L der zweiten und dritten Classe *convergiren* dann für *alle positiven* Werthe von s und sind nebst ihren Derivirten auch *stetige* Functionen des positiven Exponenten s.

Um dies nachzuweisen, betrachten wir zunächst die ganze rationale Function

$$f(x) = \Sigma\, \theta^{\alpha}\, \eta^{\beta}\, \omega^{\gamma}\, \omega'^{\gamma'} \ldots x^{\nu}$$

der Variabelen x, wo das Summenzeichen sich auf diejenigen $\varphi(k)$ positiven ganzen Zahlen ν bezieht, die relative Primzahlen zu k und $< k$ sind, und wo $\alpha, \beta, \gamma, \gamma' \ldots$ die Indices der Zahl ν bedeuten. Setzt man $x = 1$, so erhält man

$$f(1) = \Sigma\, \theta^{\alpha}\, \eta^{\beta}\, \omega^{\gamma}\, \omega'^{\gamma'} \ldots,$$

worin die Indices $\alpha, \beta, \gamma, \gamma' \ldots$ unabhängig von einander vollständige Restsysteme resp. in Bezug auf die Moduln $a, b, c, c' \ldots$ durchlaufen müssen; es ist daher

$$f(1) = \Sigma\, \theta^{\alpha} . \Sigma\, \eta^{\beta} . \Sigma\, \omega^{\gamma} . \Sigma\, \omega'^{\gamma'} \ldots$$

Da nun nach unserer Voraussetzung die Reihe L eine Reihe der zweiten oder dritten Classe, und folglich mindestens eine der Einheitswurzeln $\theta, \eta, \omega, \omega' \ldots$ *nicht* $= + 1$ ist, so ist auch mindestens eine der Summen

$$\Sigma\, \theta^{\alpha}, \quad \Sigma\, \eta^{\beta}, \quad \Sigma\, \omega^{\gamma}, \quad \Sigma\, \omega'^{\gamma'} \ldots$$

gleich Null, und hieraus folgt

$$f(1) = 0.$$

Mit Hülfe dieses Resultates kann man nun die oben behaupteten Eigenschaften der Reihen L auf verschiedene Arten nachweisen. Die eine besteht darin, dass man die Reihe L in ein bestimmtes Integral verwandelt. Nach der von *Legendre* eingeführten Bezeichnung ist

$$\Gamma(s) = \int_0^1 \left(\log \frac{1}{x}\right)^{s-1} dx$$

eine für alle positiven Werthe von s endliche und stetige Function von s; bedeutet ferner n irgend einen positiven Werth, und ersetzt man x durch x^n, so ergiebt sich

$$\frac{\Gamma(s)}{n^s} = \int_0^1 x^{n-1} \left(\log \frac{1}{x}\right)^{s-1} dx;$$

und hieraus folgt leicht (ähnlich wie in den §§. 103, 105), dass die Summe der *ersten* $m\varphi(k)$ Glieder der Reihe L gleich

$$\frac{1}{\Gamma(s)} \int_0^1 \frac{1}{x} \frac{f(x)}{1 - x^k} \left(\log \frac{1}{x}\right)^{s-1} (1 - x^{mk})\, dx$$

ist. Da nun $f(x)$ eine durch x theilbare ganze Function von x ist, welche für $x = 1$ verschwindet, so bleibt innerhalb des ganzen Integrationsgebietes der Modulus der Function

$$\frac{1}{x} \frac{f(x)}{1 - x^k}$$

unterhalb einer angebbaren endlichen Grösse, und hieraus folgt leicht, wenn man m unendlich wachsen lässt, dass

$$L = \frac{1}{\Gamma(s)} \int\limits_0^1 \frac{1}{x} \frac{f(x)}{1-x^k} \left(\log \frac{1}{x}\right)^{s-1} dx$$

ist. Es zeigt sich also in der That, dass die unendliche Reihe L der zweiten oder dritten Classe, wenn ihre Glieder in der angegebenen Weise geordnet sind, für jeden positiven Werth von s *convergirt*; beachtet man ferner, dass $\Gamma(s)$ für alle positiven Werthe von s ebenfalls positiv und von Null verschieden, sowie, dass die Derivirte von $\Gamma(s)$ eine stetige Function von s ist, so folgt aus dem vorstehenden geschlossenen Ausdruck für die Reihe L, dass dieselbe nebst ihrer Derivirten eine *stetige* Function von s ist, so lange s positiv bleibt.

Zu demselben Resultate gelangt man aber auch auf anderm Wege, nämlich mit Hülfe des weiter unten in §. 143 bewiesenen allgemeinen Satzes. Denn da zufolge der Gleichung $f(1) = 0$ die Summe der Coefficienten

$$\theta^\alpha \eta^\beta \omega^\gamma \omega'^{\gamma'} \dots$$

von je $\varphi(k)$ auf einander folgenden Gliedern der Reihe L den Werth Null hat, so bildet sowohl der reelle als auch der imaginäre Bestandtheil der Reihe L eine solche unendliche Reihe, wie sie in §. 143 betrachtet wird; man braucht dort nur $\sigma = 0$ zu setzen, und unter $g_1, g_2, g_3 \dots$ die reciproken Werthe der successiven Zahlen n zu verstehen, so ergeben sich unmittelbar unsere obigen Behauptungen über die Convergenz und Stetigkeit der Reihe L und ihrer Derivirten.

Aus diesem Resultat ergiebt sich nun, dass jede Reihe L der zweiten oder dritten Classe, wenn der Exponent $s = 1 + \varrho$ abnehmend dem Werth 1 unendlich nahe kommt, sich einem völlig bestimmten *endlichen* Grenzwerth, nämlich dem Werth

$$\int\limits_0^1 \frac{1}{x} \frac{f(x)}{1-x^k} dx$$

nähert, welchen die Reihe L bei der oben angegebenen Anordnung ihrer Glieder für $s = 1$ annimmt.

§. 135.

Es hat nun zwar gar keine Schwierigkeit, den Werth des vorstehenden Integrals mit Hülfe von Logarithmen und Kreisfunctionen darzustellen*); dass aber dieser endliche Grenzwerth einer Reihe L der zweiten oder dritten Classe *von Null verschieden* ist — und gerade hierin besteht der Hauptpunct der ganzen nachfolgenden Untersuchung — würde sich aus diesem Ausdrucke schwer oder gar nicht erkennen lassen. Es ist nun von dem höchsten Interesse, dass dieser Nachweis für die Reihen L_2 der zweiten Classe sich mit Hülfe der Untersuchungen des fünften Abschnitts über die Classenanzahl der quadratischen Formen führen lässt; ja wir können hinzufügen, dass historisch jene Untersuchungen ihren Ausgangspunct an dieser Stelle genommen haben.

Wir betrachten eine bestimmte Reihe L_2 der zweiten Classe, welche den Wurzeln

$$\theta = \pm 1, \quad \eta = \pm 1, \quad \omega = \pm 1, \quad \omega' = \pm 1 \ldots$$

entspricht; es sei P das Product aller der in k aufgehenden ungeraden Primzahlen p, denen eine negative Wurzel $\omega = -1$ entspricht, und S das Product der übrigen in k aufgehenden ungeraden Primzahlen (falls in der einen oder andern dieser beiden Gruppen gar keine Primzahl enthalten sein sollte, ist P oder $S = 1$ zu setzen); da nun eine Zahl n quadratischer Rest oder Nichtrest einer Primzahl ist, je nachdem ihr Index γ gerade oder ungerade ist (§. 129), so leuchtet ein, dass

$$\omega^{\gamma} \omega'^{\gamma'} \ldots = \left(\frac{n}{P}\right)$$

ist; wenn ferner $\theta = -1$, also $a = 2$, und $k \equiv 0 \pmod{4}$ ist, so sind alle Zahlen n ungerade, und es ist (nach §. 130)

$$\theta^{\alpha} = (-1)^{\alpha} = (-1)^{\frac{1}{2}(n-1)};$$

*) Bei der wirklichen Ausführung der Rechnung durch Zerlegung in Partialbrüche (ähnlich wie in den §§. 103, 105) würde man auf die in der Theorie der Kreistheilung vorkommenden Summen $f(r)$ stossen, wo r irgend eine Wurzel der Gleichung $r^k = 1$ bedeutet.

ebenso, wenn $\eta = -1$, also $b > 1$, und $k \equiv 0 \pmod{8}$ ist, so sind alle Zahlen n ungerade, und es ist (nach §. 130)

$$\eta^\beta = (-1)^\beta = (-1)^{\frac{1}{8}(n^2-1)}.$$

Diese Bemerkungen veranlassen uns (vergl. §§. 101, 123), je nach den vier verschiedenen Zeichencombinationen θ, η vier verschiedene Determinanten D zu betrachten; wir setzen nämlich, mit gehöriger Rücksicht auf das Zeichen ± 1:

$$\begin{aligned}
D &= \pm\ PS^2 \equiv 1 \pmod{4}, \quad \text{wenn } \theta = +1, \quad \eta = +1\\
D &= \pm\ PS^2 \equiv 3 \pmod{4}, \quad \text{wenn } \theta = -1, \quad \eta = +1\\
D &= \pm 2PS^2 \equiv 2 \pmod{8}, \quad \text{wenn } \theta = +1, \quad \eta = -1\\
D &= \pm 2PS^2 \equiv 6 \pmod{8}, \quad \text{wenn } \theta = -1, \quad \eta = -1.
\end{aligned}$$

Nun sind alle ungeraden Zahlen n auch relative Primzahlen zu $2D$, und umgekehrt, alle relativen Primzahlen zu $2D$ sind auch ungerade Zahlen n, und gleichzeitig ist

$$\theta^\alpha \eta^\beta \omega^\gamma \omega'^{\gamma'} \ldots = \theta^{\frac{1}{2}(n-1)} \eta^{\frac{1}{8}(n^2-1)} \left(\frac{n}{P}\right) = \left(\frac{D}{n}\right);$$

ist daher k gerade, so stimmen die sämmtlichen Zahlen n mit den sämmtlichen relativen Primzahlen zu $2D$ überein, und es ist

$$L_2 = \Sigma\, \psi(n) = \Sigma \left(\frac{D}{n}\right) \frac{1}{n^s};$$

ist aber k ungerade, so sind unter den Zahlen n auch gerade Zahlen; da in diesem Falle aber nothwendig $\theta = +1$, $\eta = +1$, also $D \equiv 1 \pmod{4}$ ist, so ist (vergl. §. 102)

$$L_2 = \Sigma \left(\frac{n}{P}\right) \frac{1}{n^s} = \frac{1}{1 - \left(\frac{2}{P}\right) \frac{1}{2^s}}\, \Sigma \left(\frac{D}{n}\right) \frac{1}{n^s},$$

wo in der letzten Summe rechter Hand der Buchstabe n nur noch alle ungeraden relativen Primzahlen zu k, d. h. alle relativen Primzahlen zu $2D$ zu durchlaufen hat.

Um daher zu beweisen, dass die Reihe L_2 sich einem von Null verschiedenen Grenzwerth nähert, braucht man dasselbe nur von der Reihe

$$\Sigma \left(\frac{D}{n}\right) \frac{1}{n^s}$$

nachzuweisen. Nun leuchtet ein, dass die Zahl D nie eine *Quadratzahl* sein kann; denn da eine Quadratzahl niemals $\equiv 3 \pmod{4}$, oder $\equiv 2 \pmod{8}$ oder $\equiv 6 \pmod{8}$ ist, so bleibt nur die einzige Möglichkeit $D \equiv 1 \pmod{4}$; da aber in diesem Fall $\theta = +1$, $\eta = +1$ ist, so muss, da L_2 eine Reihe der zweiten Classe ist, wenigstens eine der Wurzeln $\omega, \omega' \ldots = -1$ sein, und folglich P mindestens durch eine ungerade Primzahl p theilbar, also nicht $= 1$ sein; mithin ist D in keinem Fall eine Quadratzahl. Wir haben nun (in §§. 96 und 98) gesehen, dass die Anzahl h der Classen nicht äquivalenter ursprünglicher Formen von der (nicht quadratischen) Determinante D ein Product aus mehreren Factoren ist, von denen der eine der Grenzwerth der obigen Reihe

$$\Sigma \left(\frac{D}{n}\right) \frac{1}{n^s}$$

ist; da nun immer mindestens eine Form $(1, 0, -D)$ existirt, also h niemals $= 0$ ist, und da ferner die übrigen in dem Ausdruck von h vorkommenden Factoren nicht unendlich gross sind, so ist auch dieser Grenzwerth von Null verschieden. Und hieraus folgt, dass auch der Grenzwerth einer jeden Reihe L_2 der zweiten Classe ein von Null verschiedener und folglich positiver Werth ist, was zu beweisen war.

In dem einfachsten Fall, wo k eine Potenz einer ungeraden Primzahl p oder das Doppelte einer solchen Potenz ist, existirt nur eine Reihe

$$L_2 = \Sigma \left(\frac{n}{p}\right) \frac{1}{n^s}$$

der zweiten Classe; in diesem Fall bedarf es nicht der Zuziehung der Theorie der quadratischen Formen, um nachzuweisen, dass der Grenzwerth

$$\Sigma \left(\frac{n}{p}\right) \frac{1}{n}$$

dieser Reihe von Null verschieden ist; für diese Summe haben wir nämlich in §. 103 einen Ausdruck gefunden, welcher neben solchen Factoren, die offenbar von Null verschieden sind, noch den Factor

$$\Sigma \left(\frac{m}{p}\right) m \text{ oder } \Sigma \left(\frac{m}{p}\right) \log \sin \frac{m\pi}{p}$$

enthält, je nachdem $p \equiv 3$ oder $\equiv 1 \pmod{4}$ ist, und wo m alle Zahlen $1, 2, 3 \ldots (p-1)$ durchlaufen muss. Im ersten Fall ist aber Σm und folglich auch $\sum \left(\frac{m}{p}\right) m$ ungerade, also von Null verschieden; im zweiten Fall ist

$$-\sum \left(\frac{m}{p}\right) \log \sin \frac{m\pi}{p} = \log \frac{y + z\sqrt{p}}{y - z\sqrt{p}},$$

wo die ganzen Zahlen y, z der Gleichung $y^2 - pz^2 = 4p$ genügen; es kann folglich z, und also auch der vorstehende Ausdruck nicht $= 0$ sein.

§. 136.

Um nun dasselbe auch für jede Reihe L_3 der dritten Classe zu beweisen, addiren wir alle $\varphi(k)$ Gleichungen von der Form

$$\sum \psi(q) + \tfrac{1}{2} \sum \psi(q^2) + \tfrac{1}{3} \sum \psi(q^3) + \cdots = \log L,$$

welche den verschiedenen Wurzel-Systemen θ, η, ω, $\omega' \ldots$ entsprechen. Bedeutet q irgend eine in k nicht aufgehende Primzahl, und μ irgend eine positive ganze Zahl, so liefert die linke Seite einer jeden solchen Gleichung ein Glied $\frac{1}{\mu} \psi(q^\mu)$, in welchem

$$\frac{1}{\mu} \frac{1}{q^{\mu s}}$$

mit dem Coefficienten

$$\theta^{\alpha\mu} \eta^{\beta\mu} \omega^{\gamma\mu} \omega'^{\gamma'\mu} \ldots$$

behaftet ist, wo α, β, γ, $\gamma' \ldots$ die Indices von q bedeuten. Die Summe aller dieser den verschiedenen Wurzelsystemen θ, η, ω, $\omega' \ldots$ entsprechenden Coefficienten wird daher gleich dem Product

$$\sum \theta^{\alpha\mu} \sum \eta^{\beta\mu} \sum \omega^{\gamma\mu} \sum \omega'^{\gamma'\mu} \ldots,$$

wo die Summenzeichen sich der Reihe nach auf die a, b, c, $c' \ldots$ verschiedenen Werthe von θ, η, ω, $\omega' \ldots$ beziehen. Bekanntlich ist nun die Summe aller gleich hohen Potenzen der Wurzeln von einer Gleichung der Form $x^m = 1$ nur dann von Null verschie-

den, und zwar $= m$, wenn der Exponent dieser Potenzen durch m theilbar ist; mithin ist das vorstehende Product nur dann von Null verschieden, und zwar $= abcc' \ldots = \varphi(k)$, wenn die Exponenten $\alpha\mu$, $\beta\mu$, $\gamma\mu$, $\gamma'\mu \ldots$ resp. durch a, b, c, $c' \ldots$ theilbar sind; da nun $\alpha\mu$, $\beta\mu$, $\gamma\mu$, $\gamma'\mu \ldots$ die Indices von q^μ sind, so wird dies nur dann und immer dann eintreten, wenn

$$q^\mu \equiv 1 \ (\mathrm{mod.}\, 2^\lambda), \quad q^\mu \equiv 1 \ (\mathrm{mod.}\, p^\pi), \quad q^\mu \equiv (\mathrm{mod.}\, p'^{\pi'}) \ldots,$$

d. h. also, wenn

$$q^\mu \equiv 1 \ (\mathrm{mod.}\, k)$$

ist. Mithin wird die Summe aller jener Gleichungen folgende Form annehmen

$$\varphi(k) \left\{ \Sigma \frac{1}{q^s} + \tfrac{1}{2} \Sigma \frac{1}{q^{2s}} + \cdots + \frac{1}{\mu} \Sigma \frac{1}{q^{\mu s}} + \cdots \right\}$$
$$= \log L_1 + \Sigma \log L_2 + \Sigma \log (L_3 L'_3),$$

wo auf der linken Seite das erste, zweite Summenzeichen u. s. f. sich auf alle die in k nicht aufgehenden Primzahlen q bezieht, welche resp. den Bedingungen $q \equiv 1$, $q^2 \equiv 1 \ (\mathrm{mod.}\, k)$ u. s. f. Genüge leisten; auf der rechten Seite bezieht sich das erste Summenzeichen auf alle Reihen L_2 der zweiten Classe, das zweite auf alle verschiedenen Paare $L_3\ L'_3$ conjugirter Reihen dritter Classe. Mit Hülfe dieser Gleichung sind wir im Stande zu beweisen, dass der endliche Grenzwerth, welchem sich irgend eine Reihe L_3 der dritten Classe nähert, von Null verschieden ist.

Dieser Beweis stützt sich auf das schon früher (§. 134) erhaltene Resultat, dass jede solche Reihe L_3 für alle positiven Werthe von s eine stetige Function von s ist, und dass dasselbe auch von ihrer Derivirten gilt. Wir können daher

$$L_3 = f(s) + iF(s)$$
$$L'_3 = f(s) - iF(s)$$

setzen, wo $f(s)$, $F(s)$ und die Derivirten $f'(s)$, $F'(s)$ stetige Functionen von s sind, so lange s positiv bleibt; da also der Grenzwerth von $L_3 = f(1) + iF(1)$ ist, so muss, falls derselbe $= 0$ ist, nothwendig $f(1) = 0$ und $F(1) = 0$ sein; hieraus folgt nach einem bekannten Satze der Differentialrechnung, dass für jeden Werth $s = 1 + \varrho$, welcher > 1 ist,

$$L_3 = \varrho \left\{ f'(1 + \delta\varrho) + iF'(1 + \varepsilon\varrho) \right\}$$

$$L'_3 = \varrho \left\{ f'(1 + \delta\varrho) - iF'(1 + \varepsilon\varrho) \right\}$$

sein wird, wo δ und ε zwischen den Grenzen 0 und 1 liegen; mithin wird

$$L_3 L'_3 = \varrho^2 \left\{ f'(1 + \delta\varrho)^2 + F'(1 + \varepsilon\varrho)^2 \right\} = \varrho^2 R,$$

wo R (in Folge der Endlichkeit und Stetigkeit der Derivirten $f'(s)$, $F'(s)$] mit unendlich abnehmendem positiven ϱ sich einem endlichen (nicht negativen) Grenzwerth

$$f'(1)^2 + F'(1)^2$$

nähert. Hieraus folgt nun

$$\log (L_3 L'_3) = -2 \log \frac{1}{\varrho} + \log R,$$

wo $\log R$ mit unendlich abnehmendem ϱ sich entweder einem endlichen Grenzwerth nähert oder negativ über alle Grenzen wächst, falls R unendlich klein wird.

Sind im Ganzen m solche Paare von Reihen dritter Classe vorhanden, welche gleichzeitig mit ϱ unendlich klein werden, so ist folglich

$$\Sigma \log (L_3 L'_3) = -2m \log \frac{1}{\varrho} + t,$$

wo t jedenfalls nicht positiv über alle Grenzen wachsen kann, sondern entweder endlich bleibt, oder negativ über alle Grenzen wächst; denn da jedes Product $L_3 L'_3$ sich einem endlichen nicht negativen Werth nähert, so kann auch kein Glied $\log (L_3 L'_3)$ positiv über alle Grenzen wachsen.

Da ferner schon gezeigt ist, dass der Grenzwerth einer jeden Reihe L_2 der zweiten Classe von Null verschieden ist, so nähert sich die Summe

$$\Sigma \log L_2$$

der (jedenfalls reellen) Reihen $\log L_2$ einem endlichen Grenzwerth.

Ausserdem ist schon bewiesen, dass das Product ϱL_1 sich einem endlichen von Null verschiedenen Werth nähert; mithin ist

$$\log L_1 = \log \frac{1}{\varrho} + t',$$

wo t' endlich bleibt; folglich ist die ganze rechte Seite der obigen Gleichung von der Form

$$-(2m-1) \log \frac{1}{\varrho} + T,$$

wo T mit unendlich abnehmendem ϱ jedenfalls nicht positiv über alle Grenzen wachsen kann. Existirte also mindestens eine Reihe L_3 dritter Classe, welche mit ϱ unendlich klein würde, d. h. wäre m mindestens $= 1$, so würde die ganze rechte Seite unserer Gleichung mit unendlich abnehmendem positiven ϱ *negativ* unendlich wachsen. Dies ist aber unmöglich, da die linke Seite für alle Werthe von ϱ positiv bleibt. Mithin ist $m = 0$, d. h. jede Reihe der dritten Classe nähert sich einem von Null verschiedenen Grenzwerth, was zu beweisen war.

Hieraus folgt endlich noch, dass auch jede der Reihen $\log L_3$ einen endlichen Grenzwerth haben muss, wenn man berücksichtigt, dass nach dem früher Bewiesenen (§. 133) jede solche Reihe sich stetig mit s ändert, so lange $s > 1$ ist.

§. 137.

Das Resultat der vorhergehenden Untersuchungen besteht darin, dass bei dem unendlichen Abnehmen der positiven Grösse $\varrho = s - 1$ die Reihe $\log L_1$ positiv über alle Grenzen wächst, während alle übrigen Reihen $\log L$ sich endlichen Grenzwerthen nähern. Mit Hülfe desselben sind wir im Stande, den Satz über die arithmetische Progression vollständig zu beweisen.

Es sei nämlich m irgend eine relative Primzahl zu k, so multipliciren wir jede der $\varphi(k)$ Reihen von der Form

$$\Sigma\, \psi(q) + \tfrac{1}{2} \Sigma\, \psi(q^2) + \tfrac{1}{3} \Sigma\, \psi(q^3) + \cdots = \log L,$$

welche einem bestimmten System von Einheits-Wurzeln θ, η, ω, ω' ... entspricht, mit dem correspondirenden Werth

$$\theta^{-\alpha_1}\, \eta^{-\beta_1}\, \omega^{-\gamma_1}\, \omega'^{-\gamma_1'} \ldots = \chi,$$

wo α_1, β_1, γ_1, γ_1' ... die Indices der Zahl m bedeuten, und addiren alle Producte; dann wird, wenn wieder α, β, γ, γ' ... die

Indices einer bestimmten Primzahl q sind, das Glied

$$\frac{1}{\mu}\frac{1}{q^{\mu s}}$$

den Coefficienten

$$\Sigma\, \theta^{\alpha\mu-\alpha_1}\, \eta^{\beta\mu-\beta_1}\, \omega^{\gamma\mu-\gamma_1}\, \omega'^{\gamma'\mu-\gamma_1'}\ \ldots$$

erhalten, wo sich das Summenzeichen auf alle $\varphi(k)$ Wurzel-Systeme bezieht; dieser Coefficient ist daher auch gleich dem Product aus den einzelnen Summen

$$\Sigma\, \theta^{\alpha\mu-\alpha_1},\ \Sigma\, \eta^{\beta\mu-\beta_1},\ \Sigma\, \omega^{\gamma\mu-\gamma_1},\ \Sigma\, \omega'^{\gamma'\mu-\gamma_1'}\ \ldots,$$

in welchen die Buchstaben $\theta, \eta, \omega, \omega' \ldots$ resp. ihre $a, b, c, c' \ldots$ verschiedenen Werthe durchlaufen müssen; dieser Coefficient wird folglich nur dann von Null verschieden, und zwar $= abcc' \ldots = \varphi(k)$ sein, wenn die Exponenten $\alpha\mu - \alpha_1$, $\beta\mu - \beta_1$, $\gamma\mu - \gamma_1$, $\gamma'\mu - \gamma_1' \ldots$ resp. durch $a, b, c, c' \ldots$ theilbar sind, d. h. wenn

$$q^\mu \equiv m \text{ (mod. } k)$$

ist. Die Summation aller Producte $\chi \log L$ giebt daher das Resultat

$$\varphi(k) \left\{ \Sigma \frac{1}{q^s} + \tfrac{1}{2} \Sigma \frac{1}{q^{2s}} + \tfrac{1}{3} \Sigma \frac{1}{q^{3s}} + \cdots \right\}$$
$$= \Sigma\, \chi \log L,$$

wo auf der linken Seite das erste, zweite, dritte Summenzeichen u. s. f. sich auf alle Primzahlen q bezieht, welche resp. den Bedingungen $q \equiv m$, $q^2 \equiv m$, $q^3 \equiv m$ (mod. k) u. s. f. genügen, während das Summenzeichen auf der rechten Seite sich auf die sämmtlichen $\varphi(k)$ verschiedenen Wurzel-Systeme $\theta, \eta, \omega, \omega' \ldots$ bezieht. Bezeichnet man nun mit z alle positiven ganzen Zahlen mit Ausnahme von 1, so ist offenbar

$$\tfrac{1}{2} \Sigma \frac{1}{q^{2s}} + \tfrac{1}{3} \Sigma \frac{1}{q^{3s}} + \tfrac{1}{4} \Sigma \frac{1}{q^{4s}} + \cdots = Q$$

kleiner als

$$\tfrac{1}{2} \Sigma \frac{1}{z^2} + \tfrac{1}{2} \Sigma \frac{1}{z^3} + \tfrac{1}{2} \Sigma \frac{1}{z^4} + \cdots,$$

wo in jeder Summe z alle seine Werthe durchläuft; da nun, sobald $z \geqq 2$, immer

$$\frac{1}{z^3} \leqq \frac{1}{2}\frac{1}{z^2}, \quad \frac{1}{z^4} \leqq \frac{1}{4}\frac{1}{z^2}, \quad \frac{1}{z^5} \leqq \frac{1}{8}\frac{1}{z^2} \quad \cdots$$

ist, so ergiebt sich

$$Q < \Sigma \frac{1}{z^2};$$

während daher s abnehmend sich dem Werthe 1 nähert, bleibt Q fortwährend unterhalb einer endlichen Grösse. Da ferner alle Glieder $\chi \log L$ sich endlichen Grenzwerthen nähern, mit Ausnahme des einzigen Gliedes $\log L_1$, welches über alle Grenzen wächst, so muss auch die Summe

$$\Sigma \frac{1}{q^s}$$

über alle Grenzen wachsen; dies wäre aber nicht möglich, wenn diese Summe aus einer endlichen Anzahl von Gliedern bestände, und folglich muss es unendlich viele Primzahlen q geben, welche $\equiv m \pmod{k}$ sind; d. h. also:

Jede unbegrenzte arithmetische Progression $kx + m$, deren Anfangsglied m und Differenz k relative Primzahlen sind, enthält unendlich viele positive Primzahlen q *).

*) Ueber die Ausdehnung dieses Satzes auf Linearformen mit complexen Coefficienten, sowie auf quadratische Formen siehe: Abhandlungen der Berliner Akademie aus dem Jahre 1841; Monatsbericht der Berliner Akademie (März 1840) oder Crelle's Journal XXI; Comptes rendus der Pariser Akademie 1840, T. X, p. 285.

VII. Ueber einige Sätze aus der Theorie der Kreistheilung.

§. 138.

Sind $p, p', p'' \ldots$ positive und von einander verschiedene Primzahlen, so stimmen (nach §. 9) die Glieder des entwickelten Productes

$$(p+1)(p'+1)(p''+1) \ldots$$

mit den sämmtlichen Divisoren des Productes

$$P = pp'p'' \ldots$$

überein; dieselben Divisoren entstehen offenbar auch durch die Entwicklung des Productes

$$(p-1)(p'-1)(p''-1) \ldots,$$

aber die eine Hälfte derselben wird mit positivem, die andere mit negativem Zeichen behaftet sein; wir wollen die erstern mit δ_1, die letztern mit δ_2 bezeichnen, so dass

$$(p-1)(p'-1)(p''-1) \cdots = \Sigma\delta_1 - \Sigma\delta_2$$

wird, und wir bemerken, dass die Zahl P selbst zu der Classe der erstern gehört. Ist nun δ irgend ein Divisor von P, aber $< P$, so lässt sich leicht zeigen, dass die Anzahl der durch δ theilbaren Zahlen δ_1 genau gleich der Anzahl der durch δ theilbaren Zahlen δ_2 ist. Denn wenn man mit $q, q', q'' \ldots$ alle diejenigen Primfactoren von P bezeichnet, welche nicht in δ aufgehen, so stimmen die durch δ theilbaren Zahlen δ_1 und δ_2 resp. mit den positiven und negativen Gliedern des entwickelten Productes

$$\delta(q-1)(q'-1)(q''-1) \ldots$$

überein, und da $\delta < P$ ist, also mindestens eine solche Primzahl q vorhanden ist, so ist die Anzahl der positiven Glieder dieses Productes genau gleich der Anzahl der negativen.

Dieser Satz lässt sich leicht verallgemeinern. Bedeutet m irgend eine positive ganze Zahl > 1, und sind $p, p', p'' \ldots$ die sämmtlichen von einander verschiedenen in m aufgehenden positiven Primzahlen, so kann man

$$m\left(1-\frac{1}{p}\right)\left(1-\frac{1}{p'}\right)\left(1-\frac{1}{p''}\right)\cdots = \sum \mu_1 - \sum \mu_2$$

setzen, wo mit μ_1 und μ_2 resp. alle positiven und negativen Glieder des entwickelten Productes linker Hand bezeichnet sind. Behält man die vorhergehenden Bezeichnungen bei, so stimmen offenbar die Zahlen μ_1 und μ_2 resp. mit den Zahlen $m'\delta_1$ und $m'\delta_2$ überein, wenn zur Abkürzung $m = m'P$ gesetzt wird. Bedeutet nun μ irgend einen Divisor von m, mit Ausnahme von m selbst, so folgt hieraus wieder, dass unter den Zahlen μ_1 ebenso viele durch μ theilbar sein werden, wie unter den Zahlen μ_2. Denn, wenn μ' der grösste gemeinschaftliche Divisor von μ und m' ist, so kann man $\mu = \mu'\delta$ setzen, wo δ nothwendig ein Divisor von P, und zwar $< P$ sein muss; und da eine Zahl $\mu_1 = m'\delta_1$ oder $\mu_2 = m'\delta_2$ stets und nur dann durch $\mu = \mu'\delta$ theilbar ist, sobald resp. δ_1 oder δ_2 durch δ theilbar ist, so ergiebt sich in der That, dass die Anzahl der durch μ theilbaren Zahlen μ_1 genau gleich der Anzahl der durch μ theilbaren Zahlen μ_2 ist.

Von dieser Eigenschaft der Zahlen μ_1 und μ_2 kann man vielfache Anwendungen machen. Hängen z. B. zwei Functionen $f(m)$ und $F(m)$ einer beliebigen ganzen Zahl m durch eine der beiden Relationen

$$\sum f(\mu) = F(m)$$

oder

$$\prod f(\mu) = F(m)$$

zusammen, wo das Summen- oder Productzeichen sich jedesmal auf alle Divisoren μ (incl. m) der Zahl m bezieht, so folgt daraus resp. die Umkehrung

$$f(m) = \sum F(\mu_1) - \sum F(\mu_2)$$

oder

$$f(m) = \frac{\prod F(\mu_1)}{\prod F(\mu_2)},$$

wo die Summen- oder Productzeichen sich auf alle Werthe von μ_1 oder auf alle Werthe von μ_2 beziehen; denn ersetzt man rechts jeden Werth $F(\mu_1)$ und $F(\mu_2)$ durch die Summe oder das Product der Werthe $f(\mu)$, die den sämmtlichen Divisoren μ von μ_1 oder μ_2 entsprechen, so werden zufolge der obigen Eigenschaft der Zahlen μ_1, μ_2 alle Werthe $f(\mu)$ sich aufheben, in welchen $\mu < m$ ist, und es wird allein der Werth $f(m)$ zurückbleiben.

Als Beispiel wählen wir die Aufgabe, die Anzahl $\varphi(m)$ der ganzen Zahlen zu bestimmen, welche relative Primzahlen zu m und nicht grösser als m sind; aus dieser Definition der Function $\varphi(m)$ ist in §. 13 ohne alle Rechnung der Satz abgeleitet, dass

$$\Sigma\, \varphi(\mu) = m$$

ist, wo das Summenzeichen sich auf alle Divisoren μ von m bezieht; setzen wir daher $F(m) = m$, so ergiebt sich umgekehrt

$$\varphi(m) = \Sigma\, \mu_1 - \Sigma\, \mu_2,$$

also

$$\varphi(m) = m\left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{p'}\right)\left(1 - \frac{1}{p''}\right)\ldots;$$

diese Function ist daher durch den Satz des §. 13 schon vollständig charakterisirt.

Ein anderes Beispiel ist folgendes. Ist der Werth der Function $f(m) = p$, sobald die Zahl m eine Potenz einer Primzahl p ist, dagegen $= 1$, so oft $m = 1$ oder durch mehrere verschiedene Primzahlen theilbar ist, so leuchtet ein, dass

$$\Pi\, f(\mu) = m$$

ist, wo das Productzeichen sich auf alle Divisoren μ von m bezieht; hieraus folgt nach dem obigen Satze, dass umgekehrt der Quotient

$$\frac{\Pi\, \mu_1}{\Pi\, \mu_2} = f(m),$$

also nur dann von 1 verschieden ist, wenn m eine Potenz einer Primzahl ist; und zwar ist dieser Quotient dann gleich dieser Primzahl.

§. 139.

Die sämmtlichen Wurzeln ϱ der Gleichung

$$x^m = 1 \tag{1}$$

sind bekanntlich in der Form enthalten

$$\varrho = \cos\frac{2n\pi}{m} + i\sin\frac{2n\pi}{m},$$

wo n irgend ein vollständiges Restsystem (mod. m) durchlaufen muss.

Ist n relative Primzahl zu m, so sind die Potenzen

$$1, \varrho, \varrho^2 \ldots \varrho^{m-1}$$

sämmtlich ungleich, und sie bilden die sämmtlichen Wurzeln der obigen Gleichung (1); ϱ heisst in diesem Fall eine *primitive* Wurzel dieser Gleichung, und die Anzahl dieser primitiven Wurzeln ist offenbar $= \varphi(m)$. Ist allgemeiner ν der grösste gemeinschaftliche Divisor von n und $m = \mu\nu$, so ist ϱ eine primitive Wurzel der Gleichung

$$x^\mu = 1 \tag{2}$$

und da umgekehrt jede Wurzel der letztern Gleichung (2) auch eine Wurzel der Gleichung (1) ist, so leuchtet ein, dass die sämmtlichen Wurzeln der Gleichung (1) identisch sind mit allen primitiven Wurzeln aller der Gleichungen (2), die den sämmtlichen Divisoren μ der Zahl m entsprechen. Bezeichnet man daher mit ϱ' alle $\varphi(\mu)$ primitiven Wurzeln der Gleichung (2), und setzt

$$f(\mu) = \Pi\,(x - \varrho'),$$

wo das Productzeichen sich auf alle Wurzeln ϱ' bezieht, so ist

$$\Pi\, f(\mu) = x^m - 1,$$

wo das Productzeichen sich auf alle Divisoren μ der Zahl m bezieht; durch Umkehrung dieser für jede Zahl m geltenden Relation erhält man nach dem vorhergehenden Paragraphen

$$f(m) = \frac{\Pi\,(x^{\mu_1} - 1)}{\Pi\,(x^{\mu_2} - 1)},$$

woraus folgt, dass die Coefficienten der Function $f(m)$ sämmtlich ganze rationale Zahlen sind.

Von jetzt an betrachten wir nur noch den Fall, in welchem $m = P = pp'p'' \ldots$ eine ungerade und durch kein Quadrat theilbare ganze Zahl > 1 ist. Dann wird

$$\varphi(P) = (p-1)(p'-1)(p''-1)\ldots = \Sigma \mu_1 - \Sigma \mu_2$$

eine gerade Zahl, die wir mit 2τ bezeichnen wollen, und die sämmtlichen 2τ relativen Primzahlen zu P, welche $< P$ sind, zerfallen in τ Zahlen a und in τ Zahlen b von der Beschaffenheit, dass

$$\left(\frac{a}{P}\right) = +1, \quad \left(\frac{b}{P}\right) = -1$$

ist (§. 52. I. oder Supplemente §. 116). Setzen wir daher

$$\theta = \cos\frac{2\pi}{P} + i\sin\frac{2\pi}{P} = e^{\frac{2\pi i}{P}}$$

und

$$A(x) = \Pi(x - \theta^a), \quad B(x) = \Pi(x - \theta^b),$$

so wird

$$A(x)\,B(x) = \frac{\Pi(x^{\mu_1} - 1)}{\Pi(x^{\mu_2} - 1)},$$

und wir wollen im Folgenden die allgemeine Form der Coefficienten der Functionen $A(x)$, $B(x)$ bestimmen.

Zu diesem Zweck erinnern wir zunächst an die Newton'schen Formeln, welche dazu dienen, aus den Coefficienten einer Gleichung die Summen gleich hoher Potenzen ihrer Wurzeln, und umgekehrt aus diesen jene abzuleiten. Es seien

$$w_1, w_2 \ldots w_m$$

die Wurzeln einer Gleichung

$$x^m + c_1 x^{m-1} + c_2 x^{m-2} + \cdots + c_m = 0,$$

und

$$S_k = w_1^k + w_2^k + \cdots + w_m^k,$$

so lauten diese Formeln bekanntlich folgendermaassen:

$$S_1 + c_1 = 0$$
$$S_2 + c_1 S_1 + 2c_2 = 0$$
$$S_3 + c_1 S_2 + c_2 S_1 + 3c_3 = 0$$
$$\cdots\cdots\cdots\cdots$$
$$S_m + c_1 S_{m-1} + c_2 S_{m-2} + \cdots + c_{m-1} S_1 + m c_m = 0.$$

Aus der Form derselben geht hervor, dass $S_1, S_2 \ldots S_m$ ganze rationale Zahlen sein werden, sobald die Coefficienten $c_1, c_2 \ldots c_m$ sämmtlich ganze rationale Zahlen sind. Wenden wir dies auf die Gleichung

$$\frac{\Pi\,(x^{\mu_1} - 1)}{\Pi\,(x^{\mu_2} - 1)} = 0$$

an, so ergiebt sich, dass

$$S_k = \Sigma\,\theta^{ak} + \Sigma\,\theta^{bk}$$

für jeden Werth $k = 1, 2, 3 \ldots$ eine ganze Zahl ist. Andererseits ist nun (Supplemente §. 116)

$$\Sigma\,\theta^{ak} - \Sigma\,\theta^{bk} = \left(\frac{k}{P}\right) i^{1/4(P-1)^2} \sqrt{P},$$

und folglich

$$\Sigma\,\theta^{ak} = \tfrac{1}{2}\left(S_k + \left(\frac{k}{P}\right) i^{1/4(P-1)^2} \sqrt{P}\right)$$
$$\Sigma\,\theta^{bk} = \tfrac{1}{2}\left(S_k - \left(\frac{k}{P}\right) i^{1/4(P-1)^2} \sqrt{P}\right);$$

hiermit sind die Summen der $k$ten Potenzen der Wurzeln von jeder der beiden Gleichungen

$$A(x) = 0, \quad B(x) = 0$$

gefunden, und da dieselben keine andere Irrationalität enthalten als die Quadratwurzel

$$i^{1/4(P-1)^2} \sqrt{P},$$

so gilt zufolge der Newton'schen Formeln dasselbe von sämmtlichen Coefficienten dieser beiden Gleichungen, und zwar werden zwei gleich hohe Coefficienten in beiden Gleichungen sich nur durch das Vorzeichen dieser Quadratwurzel von einander unterscheiden, d. h. zwei solche Coefficienten werden die Formen

$$y - z\, i^{1/4(P-1)^2} \sqrt{P} \text{ und } y + z\, i^{1/4(P-1)^2} \sqrt{P}$$

haben, wo y und z rationale Zahlen bedeuten. Man kann ferner behaupten, dass y und z entweder ganze Zahlen oder Brüche mit dem Nenner 2 sind, obgleich dies aus den Newton'schen Formeln nicht unmittelbar hervorgeht; um den Beweis dieser Behauptung anzudeuten, wollen wir jede Gleichung, deren höchster Coefficient $= 1$, und deren übrige Coefficienten ganze rationale Zahlen sind, eine primäre Gleichung nennen; dann überzeugt man sich leicht, dass die Summe und Differenz zweier Wurzeln von primären Gleichungen (und ebenso ihr Product) wieder Wurzeln von primären Gleichungen sind; da nun θ die Wurzel einer primären Gleichung ist, so gilt dasselbe von jedem Coefficienten der Functionen $A(x)$ und $B(x)$ und folglich auch von

$$2y \text{ und } 2z\, i^{1/4(P-1)^2} \sqrt{P},$$

und hieraus folgt sogleich, dass die rationalen Zahlen $2y$ und $2z$ *ganze* Zahlen sein müssen.

Fasst man dies zusammen, so ergiebt sich, dass man gleichzeitig

$$2A(x) = Y(x) - Z(x)\, i^{1/4(P-1)^2} \sqrt{P}$$
$$2B(x) = Y(x) + Z(x)\, i^{1/4(P-1)^2} \sqrt{P}$$

setzen kann, wo $Y(x)$ und $Z(x)$ ganze Functionen bedeuten, deren sämmtliche Coefficienten ganze rationale Zahlen sind*). Multiplicirt man die beiden Gleichungen mit einander, so erhält man

$$Y(x)^2 - \left(\frac{-1}{P}\right) P\, Z(x)^2 = 4\, \frac{\Pi\,(x^{\mu_1} - 1)}{\Pi\,(x^{\mu_2} - 1)}.$$

§. 140.

Wir bemerken nun noch, dass man immer nur die Hälfte der Coefficienten von $Y(x)$ und $Z(x)$ zu berechnen braucht. Es ist nämlich

$$x^\tau A\left(\frac{1}{x}\right) = \Pi\,(1 - \theta^a x) = (-1)^\tau\, \theta^{\Sigma a}\, \Pi\,(x - \theta^{-a})$$

*) *Disquisitiones Arithmeticae* art. 357.

$$x^\tau B\left(\frac{1}{x}\right) = \Pi\,(1 - \theta^b x) = (-1)^\tau\,\theta^{\Sigma b}\,\Pi\,(x - \theta^{-b});$$

nun ist, je nachdem $P \equiv 1$, oder $P \equiv 3 \pmod{4}$ ist,

$$\left(\frac{-1}{P}\right) = +1, \quad \text{oder} \quad \left(\frac{-1}{P}\right) = -1,$$

und folglich

$$\Pi\,(x - \theta^{-a}) = A(x), \quad \Pi\,(x - \theta^{-b}) = B(x)$$

oder

$$\Pi\,(x - \theta^{-a}) = B(x), \quad \Pi\,(x - \theta^{-b}) = A(x);$$

ist ferner P nicht $= 3$, also $\tau > 1$, so existirt unter den Zahlen a eine von 1 verschiedene Zahl a', und da die Reste der Producte aa' mit den Zahlen a, und die Reste der Producte ba' mit den Zahlen b im Complex übereinstimmen, so ist

$$a' \sum a \equiv \sum a, \quad a' \sum b \equiv \sum b \pmod{P}$$

und folglich

$$\sum a \equiv 0, \quad \sum b \equiv 0 \pmod{P},$$

also

$$\theta^{\Sigma a} = 1, \quad \theta^{\Sigma b} = 1.$$

Mithin ergiebt sich (da τ gerade, sobald $P \equiv 1 \pmod{4}$)

$$\left.\begin{aligned} A(x) &= x^\tau A\left(\frac{1}{x}\right) \\ B(x) &= x^\tau B\left(\frac{1}{x}\right) \end{aligned}\right\}, \text{ wenn } P \equiv 1 \pmod{4}$$

und, mit Ausnahme von $P = 3$,

$$\left.\begin{aligned} A(x) &= (-x)^\tau B\left(\frac{1}{x}\right) \\ B(x) &= (-x)^\tau A\left(\frac{1}{x}\right) \end{aligned}\right\}, \text{ wenn } P \equiv 3 \pmod{4},$$

und hieraus

$$\left.\begin{aligned} Y(x) &= x^\tau\,Y\left(\frac{1}{x}\right) \\ Z(x) &= x^\tau\,Z\left(\frac{1}{x}\right) \end{aligned}\right\}, \text{ wenn } P \equiv 1 \pmod{4}$$

und, mit Ausnahme von $P = 3$,

$$\left.\begin{aligned} Y(x) &= (-x)^{\tau}\, Y\left(\frac{1}{x}\right) \\ Z(x) &= (-x)^{\tau}\, Z\left(\frac{1}{x}\right) \end{aligned}\right\}, \text{ wenn } P \equiv 3 \pmod{4}.$$

Diese Gleichungen enthalten Relationen zwischen je zwei gleich weit vom Anfang und Ende abstehenden Coefficienten der Functionen $Y(x)$ und $Z(x)$.

Die wirkliche Berechnung der Coefficienten der beiden Functionen

$$\begin{aligned} Y(x) &= y_0 x^{\tau} + y_1 x^{\tau-1} + \cdots + y_{\tau} \\ Z(x) &= z_0 x^{\tau} + z_1 x^{\tau-1} + \cdots + z_{\tau} \end{aligned}$$

geschieht nun auf folgende Art. Zuerst bildet man die Potenzsummen

$$S_k = \Sigma\, \theta^{ak} + \Sigma\, \theta^{bk}$$

für $k = 1, 2, 3 \ldots$ bis zu $\frac{1}{2}\tau$ oder $\frac{1}{2}(\tau - 1)$, je nachdem τ gerade oder ungerade ist; dies kann nach dem Obigen dadurch geschehen, dass man ebenso viele Coefficienten der ganzen Function

$$\frac{\Pi\, (x^{\mu_1} - 1)}{\Pi\, (x^{\mu_2} - 1)}$$

vom höchsten an gerechnet durch wirkliche Division bestimmt, und dann die Newton'schen Formeln anwendet; indessen hält es nicht schwer, durch Betrachtungen, welche ebenfalls auf der im §. 138 bewiesenen Haupteigenschaft der Zahlen μ_1 und μ_2 beruhen, folgende Regel abzuleiten: es sei Q der grösste gemeinschaftliche Divisor von k und $P = QR$ und r die Anzahl der in R aufgehenden Primzahlen, so ist *)

$$S_k = (-1)^r\, \varphi(Q).$$

*) Allgemeiner lautet diese Regel so: ist $m = m'P$ eine beliebige positive ganze Zahl, P das Product aus allen von einander verschiedenen in m aufgehenden Primzahlen, und S_k die Summe der $k$ten Potenzen aller primitiven Wurzeln der Gleichung $x^m = 1$, so ist $S_k = 0$, so oft k nicht durch m' theilbar ist; ist aber $k = m'K$, ferner Q der grösste gemeinschaftliche Divisor von K und $P = QR$, und r die Anzahl der in R aufgehenden Primzahlen, so ist

$$S_k = (-1)^r\, m'\varphi(Q).$$

Nachdem diese Werthe S_k gefunden sind, erhält man die Coefficienten der Functionen $Y(x)$ und $Z(x)$ durch die beiden aus den Newton'schen Formeln abgeleiteten Recursionsgleichungen

$$2ky_k = \left\{ \begin{array}{l} -\left[S_k y_0 + S_{k-1} y_1 + \cdots + S_1 y_{k-1}\right] \\ +\left(\frac{-1}{P}\right) P \left[\left(\frac{k}{P}\right) z_0 + \left(\frac{k-1}{P}\right) z_1 + \cdots + \left(\frac{1}{P}\right) z_{k-1}\right] \end{array} \right\}$$

$$2kz_k = \left\{ \begin{array}{l} +\left[\left(\frac{k}{P}\right) y_0 + \left(\frac{k-1}{P}\right) y_1 + \cdots + \left(\frac{1}{P}\right) y_{k-1}\right] \\ -\left[S_k z_0 + S_{k-1} z_1 + \cdots + S_1 z_{k-1}\right], \end{array} \right\}$$

wenn man noch berücksichtigt, dass

$$y_0 = 2, \quad z_0 = 0$$

ist.

Beispiel 1: $P = 3$; in diesem Fall müssen alle Coefficienten berechnet werden; da

$$S_1 = -1, \quad \left(\frac{1}{P}\right) = 1$$

ist, so erhält man

$$2y_1 = -S_1 y_0 = 2, \quad 2z_1 = \left(\frac{1}{P}\right) y_0 = 2,$$

und folglich

$$Y(x) = 2x + 1, \quad Z(x) = 1.$$

Beispiel 2: $P = 5$; $\tau = 2$; da wieder

$$S_1 = -1, \quad \left(\frac{1}{P}\right) = 1$$

ist, so erhält man auch wieder

$$y_1 = 1, \quad z_1 = 1,$$

und folglich

$$Y(x) = 2x^2 + x + 2, \quad Z(x) = x.$$

Beispiel 3: $P = 15 = 3 \cdot 5$; $\tau = 4$; hier ist

$$S_1 = S_2 = 1; \left(\frac{1}{P}\right) = \left(\frac{2}{P}\right) = 1; \quad \left(\frac{-1}{P}\right) = -1;$$

und folglich erhält man successive

$$y_1 = -1, \quad z_1 = 1$$

und

$$y_2 = -4, \quad z_2 = 0;$$

also ist

$$Y(x) = 2x^4 - x^3 - 4x^2 - x + 2, \quad Z(x) = x^3 - x.$$

VIII. Ueber die Pell'sche Gleichung.

§. 141.

Bedeutet D eine positive ganze Zahl, die aber kein vollständiges Quadrat ist, so ist in §. 83 durch die Betrachtung der Perioden von reducirten quadratischen Formen, die zur Determinante D gehören, nachgewiesen, dass die Pell'sche oder Fermat'sche Gleichung

$$t^2 - Du^2 = 1$$

immer unendlich viele Lösungen in ganzen positiven Zahlen t, u besitzt, und es ist dort auch eine Methode gegeben, durch welche alle diese Lösungen gefunden werden können. Es hat durchaus keine Schwierigkeit, den Zusammenhang zwischen allen diesen Lösungen zu finden, sobald nur erst der Hauptpunct bewiesen ist, dass wirklich eine Lösung existirt, in welcher u von Null verschieden ist (§. 85); *Lagrange* gebührt das Verdienst, durch Einführung neuer Principien in die Zahlentheorie diese Schwierigkeit zuerst vollständig überwunden zu haben*), und diese Principien sind später in hohem Grade verallgemeinert**). Wir wollen deshalb hier noch einen Beweis der Lösbarkeit der Pell'schen Gleichung mittheilen, welcher im Wesentlichen auf derselben Grundlage beruht.

Das Fundament dieses Beweises beruht auf der Thatsache,

---

*) Siehe die Zusätze zu der französischen Ausgabe von Euler's Algebra §§. II, VIII.

**) Vergl. drei Abhandlungen von *Dirichlet* in den Monatsberichten der Berliner Akademie vom October 1841, April 1842, März 1846; ferner die Comptes rendus der Pariser Akademie 1840, T. X, p. 286—288.

dass immer unendlich viele Paare von ganzen Zahlen x, y existiren, für welche, abgesehen vom Vorzeichen,

$$x^2 - Dy^2 < 1 + 2\sqrt{D}$$

ist; man überzeugt sich hiervon leicht, wenn man aus der Theorie der Kettenbrüche den Satz entlehnt, dass jeder Näherungswerth $\frac{x}{y}$, den man durch Entwickelung einer Grösse ω in einen Kettenbruch erhält, um weniger als $\frac{1}{y^2}$ von ω verschieden ist; nimmt man also $\omega = \sqrt{D}$, so giebt es, da $\sqrt{D}$ irrational ist, unendlich viele solche Zahlenpaare x, y, von der Beschaffenheit, dass, abgesehen vom Vorzeichen,

$$\frac{x}{y} - \sqrt{D} < \frac{1}{y^2}$$

ist; man kann daher

$$x - y\sqrt{D} = \frac{\delta}{y}$$

setzen, wo δ einen positiven oder negativen echten Bruch bedeutet. Hieraus folgt

$$x + y\sqrt{D} = \frac{\delta}{y} + 2y\sqrt{D},$$

und durch Multiplication

$$x^2 - Dy^2 = \frac{\delta^2}{y^2} + 2\delta\sqrt{D} < 1 + 2\sqrt{D}.$$

Um aber Nichts aus der Theorie der Kettenbrüche zu entlehnen, wollen wir diesen Satz noch auf einem andern und zwar ganz einfachen Wege beweisen. Es sei m irgend eine positive ganze Zahl, so legen wir der Zahl y der Reihe nach die $m + 1$ Werthe

$$0,\ 1,\ 2\ \ldots\ (m-1),\ m$$

bei, und bestimmen für jeden dieser Werthe die zugehörige ganze Zahl x durch die Bedingung

$$0 \leqq x - y\sqrt{D} < 1,$$

welche offenbar jedesmal durch eine, und nur durch eine ganze

Zahl x erfüllt wird. Theilen wir nun das Intervall von 0 bis 1 in m gleiche Intervalle von der Grösse $\frac{1}{m}$, welche durch die Werthe

$$0,\ \frac{1}{m},\ \frac{2}{m}\ \cdots\ \frac{m-1}{m},\ 1$$

begrenzt werden, so muss, da die Anzahl $m+1$ der Zahlenpaare x, y grösser ist als die Anzahl m dieser Intervalle, wenigstens eines dieser Intervalle mehr als einen, also mindestens zwei von den Werthen $x - y\sqrt{D}$ enthalten, die zwei verschiedenen Werthen von y entsprechen. Wir bezeichnen diese beiden Werthe mit $x' - y'\sqrt{D}$ und $x'' - y''\sqrt{D}$; dann ist, abgesehen vom Vorzeichen, ihr Unterschied

$$x - y\sqrt{D} = (x' - x'') - (y' - y'')\sqrt{D} < \frac{1}{m},$$

und da y', y'' nicht negativ und $\leqq m$ sind, so ist (abgesehen vom Vorzeichen) auch $y = y' - y'' < m$; setzt man nun

$$x - y\sqrt{D} = \frac{\delta}{m},$$

wo δ einen positiven oder negativen echten Bruch bedeutet, so erhält man wie oben

$$x + y\sqrt{D} = \frac{\delta}{m} + 2y\sqrt{D}$$

$$x^2 - Dy^2 = \frac{\delta^2}{m^2} + \frac{2\delta y}{m}\sqrt{D},$$

und hieraus wieder, da y absolut genommen $\leqq m$ ist,

$$x^2 - Dy^2 < 1 + 2\sqrt{D}.$$

Dass nun aber auch unendlich viele solche Zahlenpaare x, y existiren, ergiebt sich auf folgende Weise. Da y' und y'' zwei ungleiche ganze Zahlen waren, so ist $y = y' - y''$ von Null verschieden, und folglich auch $x - y\sqrt{D}$ von Null verschieden, weil $\sqrt{D}$ irrational ist; sind daher schon beliebig viele solche Zahlenpaare x, y gefunden, so kann man immer die ganze Zahl m so gross nehmen, dass $\frac{1}{m}$ kleiner wird als der kleinste der bisher

gefundenen Werthe $x - y\sqrt{D}$; für diese Zahl m erhält man aber auf die angegebene Weise wieder ein Zahlenpaar x, y von der Beschaffenheit, dass $x - y\sqrt{D} < \frac{1}{m}$ und folglich auch kleiner als alle früher gefundenen Werthe $x - y\sqrt{D}$ wird, woraus folgt, dass dieses Zahlenpaar x, y von den frühern verschieden ist; mithin ist die Anzahl dieser Zahlenpaare unbegrenzt.

§. 142.

Mit Hülfe dieses Resultates, dass immer unendlich viele Paare von ganzen Zahlen x, y existiren, für welche der absolute Werth von $x^2 - Dy^2 < 1 + 2\sqrt{D}$ und von Null verschieden wird, lässt sich nun leicht beweisen, dass die Gleichung $t^2 - Du^2 = 1$ immer in ganzen Zahlen t, u lösbar ist, und zwar so, dass u von Null verschieden ausfällt.

Da die Anzahl der ganzen Zahlen, welche, abgesehen vom Vorzeichen $< 1 + 2\sqrt{D}$ sind, endlich ist, so muss der Ausdruck $x^2 - Dy^2$ für unendlich viele Zahlenpaare x, y einer und derselben (von Null verschiedenen) Zahl k gleich werden; da ferner die Anzahl der verschiedenen Paare von Resten, welche zwei Zahlen x, y (mod. k) lassen können, endlich, nämlich $= k^2$ ist, so leuchtet ebenso ein, dass unter den unendlich vielen Zahlenpaaren x, y, für welche

$$x^2 - Dy^2 = k$$

wird, auch wieder unendlich viele Paare x, y sich finden müssen, in welchen

$$x \equiv \alpha,\ y \equiv \beta \text{ (mod. } k)$$

ist, wo α, β zwei bestimmte Reste bedeuten. Sind nun x', y' und x'', y'' irgend zwei solche Zahlenpaare, d. h. ist gleichzeitig

$$x'^2 - Dy'^2 = x''^2 - Dy''^2 = k$$

und

$$x' \equiv x'',\ y' \equiv y'' \text{ (mod. } k),$$

so bilden wir das Product

$$x + y\sqrt{D} = (x' - y'\sqrt{D})\,(x'' + y''\sqrt{D}),$$

indem wir

$$x = x'x'' - Dy'y'', \quad y = x'y'' - y'x''$$

setzen; dann ist gleichzeitig

$$x - y\sqrt{D} = (x' + y'\sqrt{D})\;(x'' - y''\sqrt{D}),$$

und hieraus ergiebt sich durch Multiplication

$$x^2 - Dy^2 = (x'^2 - Dy'^2)\,(x''^2 - Dy''^2) = k^2.$$

Da nun ausserdem

$$x = x'x'' - Dy'y'' \equiv 0 \pmod{k}$$
$$y = x'y'' - y'x'' \equiv \pmod{k}$$

ist, so können wir

$$x = tk, \; y = uk$$

setzen, wo t, u ganze Zahlen bedeuten, die der Gleichung

$$t^2 - Du^2 = 1$$

genügen; und zwar dürfen wir annehmen, dass u von Null verschieden ist; denn aus

$$y = x'y'' - y'x'' = 0$$
$$x''^2 - Dy''^2 = x'^2 - Dy'^2 = k$$

ergiebt sich

$$x'' = \pm x', \quad y'' = \pm y';$$

da aber unendlich viele solche Zahlenpaare x', y' und x'', y'' existiren, so können wir auch immer zwei solche auswählen, dass x'', y'' verschieden von $\pm x'$, $\pm y'$, und folglich u von Null verschieden ausfällt.

Hiermit ist also in der That bewiesen, dass immer eine Lösung t, u der vorstehenden Pell'schen Gleichung existirt, in welcher u von Null verschieden ist.

Hieraus lässt sich dann (wie in §. 85), ebenfalls ohne Hülfe der Theorie der reducirten Formen, zeigen, dass alle Auflösungen t, u sich aus der Gleichung

$$t + u\sqrt{D} = \pm (T + U\sqrt{D})^n$$

ergeben, wo T, U die kleinsten positiven ganzen Zahlen bedeu-

ten, die der Gleichung genügen, und der Exponent n alle positiven und negativen ganzen Zahlen durchläuft. Nur in der einen Beziehung bleibt diese Theorie der Pell'schen Gleichung unvollständig, dass aus ihr keine directe Methode fliesst, diese kleinste positive Auflösung T, U unmittelbar zu finden. Hierzu und ebenso zur Beurtheilung der Aequivalenz zweier Formen und also auch der Darstellbarkeit einer Zahl durch eine Form bleibt die Theorie der reducirten Formen unentbehrlich.

IX. Ueber die Convergenz und Stetigkeit einiger unendlichen Reihen.

§. 143.

Die Methode, welche in §. 101 angewendet ist, um die Convergenz und Stetigkeit der Reihe

$$\frac{\alpha_1}{1^s} + \frac{\alpha_2}{2^s} + \frac{\alpha_3}{3^s} + \cdots$$

zu beweisen, lässt sich leicht auf Reihen von der allgemeineren Form

$$A = \alpha_1 g_1^s + \alpha_2 g_2^s + \alpha_3 g_3^s + \cdots$$

übertragen, wo $g_1, g_2, g_3 \ldots$ positive Grössen bedeuten, welche, wenigstens von einer bestimmten Stelle ab, fortwährend abnehmen und zuletzt unendlich klein werden; man erhält auf diese Weise folgenden Satz:

Wenn für einen bestimmten Werth $s = \sigma$ die Summe von noch so vielen auf einander folgenden Gliedern der Reihe A ihrem absoluten Werth nach stets kleiner als ein bestimmter endlicher Werth C bleibt, so convergirt die Reihe A für alle Werthe $s > \sigma$ (excl. σ), und sie ist nebst allen ihren Derivirten eine stetige Function von s.

Um dies zu beweisen, setze man $s = \sigma + r$, wo also r eine positive Grösse ist, ferner

$$\beta_n = \alpha_1 g_1^\sigma + \alpha_2 g_2^\sigma + \cdots + \alpha_n g_n^\sigma,$$

und vergleiche die Reihe A mit der folgenden

$$B = \beta_1 (g_1^r - g_2^r) + \beta_2 (g_2^r - g_3^r) + \cdots,$$

so findet man, dass die Summen der n ersten Glieder beider Reihen

sich um die Grösse $\beta_n g_{n+1}^r$ von einander unterscheiden, welche, da β_n (absolut genommen) stets $< C$, und r positiv ist, mit unendlich wachsendem n unendlich klein wird, weil g_{n+1} ebenfalls unendlich klein wird. Die Reihe A wird daher mit der Reihe B gleichzeitig convergiren, oder mit ihr divergiren, und im erstern Falle haben beide Reihen denselben Werth; wir brauchen daher nur noch die Reihe B zu betrachten.

Nimmt man n so gross, dass die Werthe $g_{n+1}, g_{n+2} \dots$ fortwährend abnehmen, dass also die Differenzen

$$g_{n+1}^r - g_{n+2}^r, \quad g_{n+2}^r - g_{n+3}^r \dots$$

sämmtlich positiv sind, so ergiebt sich, dass die Summe von beliebig vielen, auf die n ersten folgenden, Gliedern der Reihe B (absolut genommen) $< C g_{n+1}^r$ ist und folglich durch die Wahl eines hinreichend grossen Werthes n beliebig klein gemacht werden kann. Mithin convergirt die Reihe B, und folglich auch die Reihe A für jeden positiven Werth r, d. h. für jeden Werth $s > \sigma$. Um ferner die Stetigkeit dieser Reihen für alle diese Werthe von s oder r zu beweisen, genügt es, alle Werthe r zu betrachten, welche $\geqq \varrho$ sind, wo ϱ irgend ein beliebig angenommener positiver Werth ist. Für alle diese Werthe ist nun die Summe aller auf die n ersten folgenden Glieder der Reihe B (absolut genommen) $< C g_{n+1}^r$, also auch $< C g_n^\varrho$, während die Summe der n ersten Glieder sich stetig mit s oder r ändert; da also durch eine zweckmässige Zerlegung der Reihe B in zwei Bestandtheile, d. h. durch die Wahl eines hinreichend grossen n, der zweite Bestandtheil für alle in Betracht kommenden Werthe r kleiner als irgend eine gegebene Grösse gemacht werden kann, während der erste Bestandtheil seiner Natur nach stetig ist, so ist auch die ganze Reihe B, und also auch die Reihe A, eine stetige Function von $s = \sigma + r$, so lange r positiv ist.

Um dieselben Behauptungen auch für die Derivirten der Reihe A zu beweisen, betrachten wir die Reihe

$$A' = \alpha_1 g_1^s \log g_1 + \alpha_2 g_2^s \log g_2 + \alpha_3 g_3^s \log g_2 + \cdots,$$

deren einzelne Glieder die Derivirten von den entsprechenden Gliedern der Reihe A sind, und vergleichen sie mit der Reihe

$$B' = \beta_1 (g_1^r \log g_1 - g_2^r \log g_2) + \beta_2 (g_2^r \log g_2 - g_3^r \log g_3) + \cdots,$$

welche auf dieselbe Weise aus der Reihe B entsteht. Bedenkt man nun, dass die Function $x^r \log x$ der positiven Variabeln x, sobald $x < 1$ und $(1 + r \log x)$ negativ geworden ist, ebenfalls negativ wird, dem absoluten Werthe nach gleichzeitig mit x abnimmt und unendlich klein wird, so erkennt man leicht, dass alle im Vorhergehenden für die Reihen A und B bewiesenen Behauptungen sich auf die Reihen A' und B' übertragen lassen; beide Reihen convergiren für jeden positiven Werth von r, haben gleiche Summen und bilden eine stetige Function von r oder $s = \sigma + r$. Es braucht daher nur noch gezeigt zu werden, dass $dB = B'dr$, oder, was dasselbe sagt, dass das Integral

$$J = \int_{\varrho}^{r} B' dr,$$

dessen untere Grenze ϱ ein beliebig gewählter positiver Werth $< r$ ist, $= B - R$ ist, wo R den Werth der Reihe B für $r = \varrho$ bedeutet. Zerlegt man nun B' in zwei Bestandtheile B'_n und $\mathfrak{B}'_n$, von denen der erstere die Summe der n ersten Glieder der Reihe B' ist, so wird

$$J = B_n - R_n + \int_{\varrho}^{r} \mathfrak{B}'_n dr,$$

wo B_n und R_n resp. die Summen der n ersten Glieder der Reihen B und R bedeuten. Da ferner, wenn n hinreichend gross genommen wird, der Bestandtheil $\mathfrak{B}'_n$ innerhalb des ganzen Integrationsgebietes absolut genommen $< C g_n^{\varrho} \log g_n$, und folglich

$$\int_{\varrho}^{r} \mathfrak{B}'_n dr < C(r - \varrho) g_n^{\varrho} \log g_n$$

ist, so leuchtet ein, dass der Unterschied zwischen dem Integrale J und der Differenz $(B_n - R_n)$ mit unendlich wachsendem n unendlich klein wird, und dass folglich $J = B - R$ ist, was zu beweisen war.

In derselben Weise kann man auch den Beweis für die Derivirten höherer Ordnung führen.

§. 144.

Wir fügen zum Schluss noch einige Bemerkungen über Reihen von der Form A oder B hinzu. Im vorhergehenden Paragraphen war angenommen, dass die positiven Grössen $g_1, g_2, g_3 \ldots$ von einer bestimmten Stelle ab fortwährend abnehmen und zuletzt unendlich klein werden. Giebt man diese letztere Voraussetzung auf, nimmt man aber immer noch an, dass diese Grössen von einer bestimmten Stelle ab fortwährend abnehmen, so muss g_n mit unendlich wachsendem n sich einem bestimmten Grenzwerth nähern, den wir mit g bezeichnen wollen.

Nehmen wir nun wieder an, dass β_n seinem absoluten Werth nach stets $< C$ bleibt, so ist die Summe von beliebig vielen, auf die n ersten folgenden, Gliedern der Reihe B absolut genommen $< C(g_n^r - g^r)$, und folglich convergirt auch jetzt noch die Reihe B für jeden positiven Werth von r, und sie ist nebst ihren Derivirten eine stetige Function von r. Die Reihe A dagegen wird für positive Werthe von r, d. h. für Werthe $s > \sigma$ stets und nur dann convergiren, wenn sie für $r = 0$, d. h. für $s = \sigma$ convergirt, also, wenn β_n mit unendlich wachsendem n sich einem Grenzwerth β nähert; und zwar ist dann $A = B + \beta g^r$ (hierin ist offenbar das frühere Resultat enthalten, wenn $g = 0$ ist). Unter dieser Voraussetzung, dass die Reihe A auch noch für $s = \sigma$ convergirt, dass also β_n mit unendlich wachsendem n sich einem Grenzwerth β nähert, ist es von Interesse, das Verhalten der Reihen A und B bei unendlichem Abnehmen der positiven Grösse r zu untersuchen. Sind β' und β'' zwei beliebige Werthe, aber so beschaffen, dass $\beta' < \beta < \beta''$ ist, so kann man n immer so gross wählen, dass für dieses n und alle noch grössern Werthe $\beta' < \beta_n < \beta''$ wird; es wird dann die Summe aller Glieder der Reihe B von dem $n$ten ab zwischen den Werthen $\beta'(g_n^r - g^r)$ und $\beta''(g_n^r - g^r)$ liegen, und da die Summe der n ersten Glieder gleichzeitig mit r unendlich klein wird, so ergiebt sich leicht, dass die Reihe B sich dem Grenzwerth β oder dem Grenzwerth Null nähern wird, je nachdem $g = 0$ oder von Null verschieden ist; da ferner der Werth der Reihe B, welcher dem Werth $r = 0$ entspricht, ebenfalls $= 0$ ist, so leuchtet ein, dass die Reihe B an dieser Stelle nur dann unstetig ist, wenn gleichzeitig $g = 0$ und

β von Null verschieden ist. Dagegen ergiebt sich aus der Gleichung $A = B + \beta g^r$, dass die Reihe A sich in allen Fällen dem Grenzwerth β nähert und folglich auch noch an dieser Stelle stetig ist.

Wir leiten endlich noch den folgenden in §. 91 benutzten Satz ab: Convergirt die Reihe A für einen bestimmten Werth $s = \sigma$ und folglich auch für jeden Werth $s > \sigma$, und sind die sämmtlichen Grössen $g_1, g_2, g_3 \ldots$ echte Brüche, so wird sowohl der Werth von A, als der von B mit unendlich wachsendem positiven s unendlich klein. Um sich hiervon zu überzeugen, braucht man nur zu bedenken, dass, wenn die Grössen $g_1, g_2, g_3 \ldots$ von g_n ab fortwährend abnehmen, die Summe aller, auf die n ersten folgenden, Glieder der Reihe B absolut genommen $< C(g_n^r - g^r)$ ist und folglich mit unendlich wachsendem positiven r unendlich klein wird; und da dasselbe von der Summe der n ersten Glieder gilt, so wird B, und folglich auch $A = B + \beta g^r$ ebenfalls unendlich klein.

Wir schliessen mit der Bemerkung, dass die vorstehenden Sätze leicht in Sätze über Potenzreihen verwandelt werden können; setzt man nämlich

$$e^{-s} = x \text{ und } g_n = e^{-\lambda_n},$$

so wird

$$A = \alpha_1 x^{\lambda_1} + \alpha_2 x^{\lambda_2} + \alpha_3 x^{\lambda_3} + \cdots,$$

wo die Exponenten $\lambda_1, \lambda_2, \lambda_3 \ldots$, wenigstens von einer bestimmten Stelle ab, fortwährend (algebraisch) zunehmen.

Das wesentliche Princip der vorhergehenden Untersuchungen, nämlich die Vergleichung der Reihe A mit der Reihe B, ist zuerst von *Abel* angewendet *).

---

*) Untersuchungen über die Binomialreihe (Crelle's Journal I).

